



## **Windows Intune** for G Cloud

*G-Cloud Service Definition Document in response to G-Cloud ITT tender –  
RM1557iii G-Cloud RFX*

## Contents

1.	AN OVERVIEW OF THE WINDOWS INTUNE SERVICE.....	3
2.	INFORMATION ASSURANCE .....	4
3.	BACK UP/RESTORE AND DISASTER RECOVERY.....	4
4.	SERVICE ARCHITECTURE.....	4
5.	ON-BOARDING AND OFF-BOARDING TO THE WINDOWS INTUNE SERVICE .....	7
6.	WINDOWS INTUNE LICENSING AND PRICING .....	7
7.	TERMINATION TERMS .....	8
8.	WINDOWS INTUNE SERVICE MANAGEMENT .....	9
9.	SERVICE LEVELS .....	11
10.	FINANCIAL RECOMPENSE MODEL FOR NOT MEETING SERVICE LEVELS .....	11
11.	WINDOWS INTUNE TRAINING .....	11
12.	TECHNICAL REQUIREMENTS.....	13
13.	DETAILS OF ANY TRIAL SERVICE AVAILABLE.....	17
14.	DATA EXTRACTION AND REMOVAL .....	18
15.	DEPLOYMENT MODELS:.....	18
	APPENDIX 1 – MICROSOFT WINDOWS INTUNE SERVICE LEVEL AGREEMENT (SLA)	19

# Service Definition

The name of the service is “Windows Intune”.

## 1. AN OVERVIEW OF THE WINDOWS INTUNE SERVICE

Windows Intune™ is a comprehensive solution that offers the powerful combination of Windows Intune cloud services and Windows software.

Windows Intune helps IT administrators keep their Windows-based PCs and mobile devices well managed and secure from virtually anywhere with cloud-based management tools, reports and an optional upgrade license to the latest version of Windows. Windows Intune enables users to more securely access targeted applications for the devices they use to get work done while on the go.

By replacing the need for multiple tools and an extensive server-based infrastructure with this easy-to-deploy cloud service, customers can:

- **Track up to the minute system health data:** Through the Web-based Admin console customers can see up to date views of the alerts and system health for all of their managed devices.
- **Identity federation:** Customers can use tools such as the Microsoft Online Services Directory Synchronization tool (DirSync) and Active Directory Federation Services (ADFS) to seamlessly integrate their local Active Directory Domain Service (AD DS) infrastructure with Windows Intune and have a single sign on experience for users both in the cloud and on-premises.
- **Protect PCs from malware:** Help protect workers’ PCs from the latest threats with centralized endpoint protection that uses the same trusted malware protection engine used in System Center Endpoint Protection 2012 and Microsoft Security Essentials.
- **Manage software updates:** Centrally manage the deployment of updates to Microsoft and most third-party software publishers, keeping the applications workers need current.
- **Distribute software:** Deploy licensed software, like Microsoft Office 2010, or many third-party applications, to PCs located nearly anywhere via the cloud.
- **User-empowerment:** Allow users to provision their own devices and install published software using the Windows Intune self-service company portal.
- **Proactively monitor PCs:** Receive alerts on updates and threats to proactively identify and help resolve problems with customer PCs virtually anywhere.
- **Provide remote support:** Resolve PC issues, regardless of where users are located, with remote assistance and remote tasks.
- **Track hardware and software inventory:** Track hardware and software assets used to efficiently manage assets.
- **Set security policies:** Centrally manage update, firewall, and endpoint protection policies, even on remote machines outside the corporate network.
- **Manage licenses:** Manage Microsoft Volume License Agreements and other license agreements, including retail, Original Equipment Manufacturer (OEM) licenses and third-party software licenses, to track how many licenses the organization has purchased against what they’ve installed.\*
- **Increase insight with reporting:** Generate and save custom reports for updates, software, hardware, and licenses. Export data as a comma separated value (CSV) file and import it directly into Microsoft Excel® or other reporting tools for further analysis.
- **Automate group membership:** Use AD DS security groups and user account membership to automatically assign Windows Intune policies, updates and software deployment rights.

- **Manage mobile devices:** Use Windows Intune to integrate and manage mobile phone and tablet devices including Windows Phone, iOS and Android devices.
- **Set mobile device security policies:** Create mobile device specific security policies to control access to communications and better protect the data on mobile device.
- **Protect data on mobile devices:** Remotely wipe personal and agency data from mobile devices if they are lost or stolen.

In order to use the core service features, the customer just needs an Internet connection and the Windows Intune client installed on each PC they wish to manage. To enable the directory integration features the customer will need to link their AD DS with Windows Intune. Integration with a customer's Microsoft Exchange infrastructure will allow them to enable the Windows Intune mobile device management features. All of these features can be used by in-house IT professionals or by solution providers to manage the PCs and mobile devices of multiple agencies. Additionally, Windows Intune can be used with the most common professional software automation (PSA) and customer relationship management (CRM) tools used by solution providers, so they can offer smooth tracking from issue to resolution.

Customers who purchase Windows Intune with Software Assurance also have the option to purchase the Microsoft Desktop Optimization Pack (MDOP) add-on, a set of six on-site advanced desktop management tools. MDOP can help further enhance security and control and help you resolve critical issues that cannot be addressed by the cloud service, such as diagnosing and recovering unbootable PCs.

## 2. INFORMATION ASSURANCE

Windows Intune is currently an IL0 service. We are working towards gaining the IL2 standard.

## 3. BACK UP/RESTORE AND DISASTER RECOVERY

The following section outlines the redundancy and failover procedures that are offered with Windows Intune.

### **Fault-Tolerance & Redundancy**

Microsoft Online Services are designed to be fault-tolerant and redundant. From geographically diverse data center deployments to clustered server farms, all aspects of the service provide for fault-tolerance and redundant service.

### **Service Redundancy**

Each layer of the infrastructure is designed to continue operations in the event of failure, including redundant network devices at each layer and dual internet service providers at each data center. The network is monitored by the Network Operations Center 24x7x365 to detect any anomalies or potential network issues.

### **Data Center Redundancy**

Microsoft data centers feature automated failover that can transfer operations to alternative, geographically separate data centers if this becomes necessary. Failover is transparent, requiring no intervention from customers while service is resumed.

More information about Microsoft data center management may be found here:

<http://www.globalfoundationservices.com/cloud-scale-data-centers.aspx>.

## 4. SERVICE ARCHITECTURE

There are five main technology components to the Windows Intune solution.

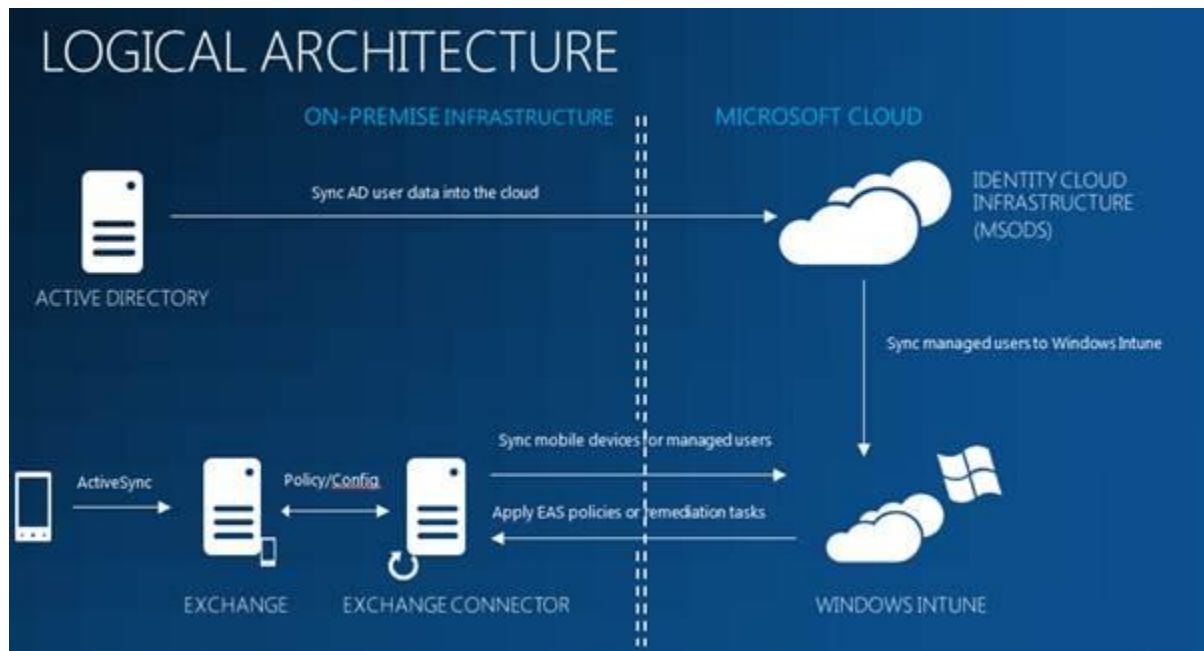
The first component is the Windows Intune service itself, which has been designed from the ground up as a highly scalable and reliable cloud-based service. The design of the Windows Intune service was based on the work that was done for the Microsoft Update Service (the world's largest cloud-based service). The geographically dispersed data centers that support this service are enterprise-class, redundant systems that support millions of customers every day.



The next component is the Windows Intune client agents, which handle the communications from managed devices to the Windows Intune service. Communications are secured and encrypted by using Secure Sockets Layer (SSL) and are initiated from the client over Port 80 and Port 443, both of which tend to work with most organizations' firewalls without additional configuration.

The third component is the Windows Intune Account Portal, which allows the customer to enroll Windows Intune devices and users, configure Active Directory synchronisation and to manage subscriptions. Windows Intune uses the same authentication mechanism as Office 365, so that the customer can integrate Windows Intune with their existing Active Directory Domain Services (AD DS) environment. Using Microsoft Online Directory Service (MSODS) to synchronise on-premise Active Directory user data with Windows Intune allows for single sign-on for both the Windows Intune administrators and Windows Intune users. This can be extended further to incorporate two-factor authentication thus increasing secure access.

By integrating Windows Intune with AD DS, the customer can synchronize existing security groups and users from AD DS to Windows Intune and manage them with Windows Intune. With Windows Intune a customer can obtain their organisation's Microsoft Online Service domain which then allows them to link that domain with their existing AD DS environment using the Microsoft Online Services Directory Synchronization tool. This tool will maintain a one-way directory synchronization of all configured user accounts and mail-enabled contacts and groups from their local AD DS to your Microsoft Online Services domain. The Exchange 2010 integration facilitates Mobile Device Management by implementing Security Policies as defined in Exchange ActiveSync (EAS) and enables the customer to run reports and help determine compliance with such policies. The EAS integration means that Windows Intune will present the actual rules as they are on Exchange. If an Exchange Administrator changes the rules, they are re-imported into Windows Intune and an alert is presented notifying Administrators of the change. This is illustrated below:



The fourth component is the Windows Intune Company Portals. This provides users with self-service capabilities, through two Web-based company portals – one for x86-based devices and one for non-x86-based mobile devices. These portals enable a customer’s users to perform common tasks without having to call the help desk. This helps reduce support costs, enables a customer’s users to be more productive, and gives their IT staff the ability to remain focused on more important tasks. The following table describes both of these portals:

Name	Description
Windows Intune Company Portal	This portal supports Windows-based computers and lets users browse applications that you make available, install applications on their computers, and manage their devices. For example, authorized users can add their computers or mobile devices to Windows Intune or remove them. For users who do need to contact their IT help desk, you can provide customized IT contact information that is suitable for your organization.  Portal address = <a href="https://portal.manage.microsoft.com">https://portal.manage.microsoft.com</a>
Windows Intune Mobile Company Portal	This version of the company portal is optimized for mobile devices. Authorized users can visit this portal, sign in to Windows Intune, browse and install internal line-of-business applications that you make available, install the applications on their mobile devices, and contact their IT Help desk.  Portal address = <a href="https://m.manage.microsoft.com">https://m.manage.microsoft.com</a>

These two portals are designed to make the process of downloading available applications as simple as possible for your users. Also, you control who can access these portals. To get users started with the service, administrators must add users to the Windows Intune service and make applications available to them before they can add or remove computers and mobile devices or install available software.

The final component is the Windows Intune IT Administrator Portal or Console, which displays data from the managed computers and devices. This console is also secured and encrypted by using SSL. Only a synchronised Active Directory account that has specifically been granted administrative rights to the account may access the Windows Intune IT Administrator Console.

Information about Windows Intune security can be found here: <http://www.microsoft.com/en-us/download/details.aspx?id=30184>.

## 5. ON-BOARDING AND OFF-BOARDING TO THE WINDOWS INTUNE SERVICE

For information about getting started with Windows Intune customers can visit the Windows Intune site [www.windowsintune.com](http://www.windowsintune.com).

The Windows Intune team can help customers to set up new trials for and support the onboarding and off boarding process to Windows Intune. Further information can be found at the 'How to buy' and 'Termination terms' sections below.

## 6. WINDOWS INTUNE LICENSING AND PRICING

Customers can license Windows Intune in either of the following ways:

- **Through Microsoft Online Customer Portal**

The Microsoft Online Customer Portal (MOCP) is the portal used to purchase Microsoft online services such as Office 365, Windows Azure, and Windows Intune. For purchases made through MOCP, the full price will be shown to the customer/partner when they make their purchase.

- **Windows Intune Volume Licensing SKUs**

Customers may purchase either the Windows Intune License or the Windows Intune Add-On for System Center Configuration Manager (ConfigMgr) and System Center Endpoint Protection (SCEP) License via the EA/EA Subscription (EAS) or EES agreements.

- Customers without an existing EA/EAS or an existing EA /EAS without ConfigMgr and SCEP may purchase the full Windows Intune SKU.
- Customers with an EA, EAS, or EES with ConfigMgr and SCEP may purchase the Windows Intune Add On SKU, allowing them to pay only for the Windows Intune service being added onto their existing agreement.

### Billing Cycle

During the subscription term, the customer will receive a monthly bill for the quantity of Device Subscription Licenses purchased for that term. Additional licenses may be added.

### Additions

- Units can be added to the subscription at any time at the current subscription purchase price.
- The added units will follow the original subscription anniversary date for renewals.
- When adding units moves the organization to a new pricing tier, all existing and new units take the lower prices of that tier from that point onward.
- New units added between billing cycles will be billed on a prorated basis in the next billing cycle.

### Reductions

- Reductions within the first 12-month subscription period are not allowed.
- If reductions after the first 12-month term move you to a new pricing tier, all your units will assume the pricing within the new tier.

## Auto Renew

Nearing the end of the subscription, the customer will be notified that their subscription is coming to an end. If no action is taken, their subscription will automatically be renewed for another 12-month term.

Opting out of the auto renewal feature can be done through MOCP. If the customer has opted out of auto renew and would like to continue the Windows Intune service when the initial subscription ends they will need to call Support to manually renew the subscription before the end of the 30-day grace period.

Subscriptions are renewed at the purchase price, unless pricing changes during the subscription term. Price protection continues throughout the renewed subscription. Microsoft retains the right to change the price by giving 30-day notice before the renewal date.

## Pricing

Windows Intune is purchased at the following price for public sector organisations. Price is per user and includes one main device (Desktop or Laptop) and up to 4 mobile devices (tablet, slate, mobile phone).

Windows Intune	£3.44
Windows Intune with Windows Software Assurance	£6.31
Windows Intune Add On for Configuration Manager	£2.29
Windows Intune Additional Storage Add On	£1.44

## Price Protection

The unit price agreed to upon subscription will stay the same throughout a customer's 12 month subscription. Microsoft reserves the right to lower the price at any time. The price will be quoted at the time of purchase.

## 7. TERMINATION TERMS

The Windows Intune service is governed by the terms and conditions of the agreement(s) under which the customer purchased the services

Termination Terms for licenses purchased through MOCP

**Cancelling a New Subscription** A customer can cancel at any time within 30 days of purchase and will be billed for the first month. Cancellations can be made after that point, but the customer will be responsible for paying for the entire initial 12-month subscription.

**Cancelling a Subsequent Subscription** After the initial 12-month subscription the customer can call to cancel any time. The cancellation will take effect at the end of the following subscription month.

**Windows Buyout Option** When customers cancel in subsequent terms (after the initial 12-month subscription) they have the ability to retain their Windows licenses by purchasing and converting them to perpetual use licenses from a License. The licenses are required to have been active for a minimum of 12 months before a customer is eligible to take advantage of the perpetual license offer.

If the customer chooses not to purchase the Windows licenses, then Windows will need to be uninstalled from their organizations computers or they will need to purchase a buyout SKU.

The licensing terms of the Windows Buy-Out option are similar to other subscription programs like Open Value Licensing.



The full terms of termination for Windows Intune can be found by going to Section 4 'Term, suspension, and termination' of the Online Subscription Agreement Terms and Conditions, this can be found [here](#).

### Termination Terms for licenses purchased through EA, EES, EAS

#### Canceling a New or Subsequent Subscription (In Initial Term)

Specific scenarios allow for reduction to a cancelled state at an anniversary.

Reductions are allowed at anniversary for Windows Intune as long as minimal program criteria are met. License reductions will result in an adjustment to future billing and will take effect upon the enrollment anniversary following the reduction.

Further information and a copy of a customer's agreement(s) can be found by contacting their Microsoft representative or clicking [here](#)

## 8. WINDOWS INTUNE SERVICE MANAGEMENT

Windows Intune has a well-defined change control process to provide applicable patches and/or upgrades. This includes deployment and verification of patches in a pre-production environment, scheduled maintenance windows for production deployment, and defined notification processes to help minimize interruption of the service. Windows Intune notifies administrators through various methods including the web console and email of scheduled or unscheduled updates and changes to the service. For planned service interrupting events (such as service maintenance), customers are notified five days in advance.





### Service Monitoring







The Windows Intune service is monitored on a 24x7 basis for reliability and performance. The data center operations group monitors the network for security vulnerabilities and intrusion using monitoring and detection systems on a continuous basis. All of the monitoring tools route any issues, warnings, and problems to service engineers.

The service has multiple layers of monitoring in place. The infrastructure/platform layer is monitored using Microsoft System Center Operations Manager (SCOM). SCOM monitors for events related to provisioning, service failures, and threshold attainment (such as memory consumption).

Windows Intune Status Health is an online service detailing up to date information regarding the Status Health of Windows Intune back-end Infrastructure. This can be found at <http://status.manage.microsoft.com/Statuspage/servicedashboard.aspx> and examples are shown below:

**Current Status** shows an up to date report of the Windows Intune Service Status. An example of current service status is shown below:

Status	Service Instance	Details
	Asia 2-01	The service instance is running normally.
	Asia 2-02	The service instance is running normally.
	Asia 2-03	The service instance is running normally.
	Europe 2-01	The service instance is running normally.

	Europe 2-02	The service instance is running normally.
	Europe 2-03	The service instance is running normally.
	North America 2-01	The service instance is running normally.
	North America 2-02	The service instance is running normally.
	North America 2-03	The service instance is running normally.
	North America 2-04	The service instance is running normally.

























































**Scheduled Maintenance Notification** details when scheduled maintenance is to occur on the Windows Intune infrastructure. An example of a Scheduled Maintenance Notification is show below:

**Scheduled Maintenance Notification**

Currently there is no scheduled maintenance

**Status History**

The service status history is maintained for five weeks. Move the pointer over the status icon to view more information when available. To scroll through the weeks, click the arrow icon at the top of the table.

Service Instance	June 19	June 18	June 17	June 16	June 15	June 14	June 13
Asia 2-01							
Asia 2-02							
Asia 2-03							
Europe 2-01							
Europe 2-02							
Europe 2-03							
North America 2-01							
North America 2-02							 <div style="border: 1px solid black; padding: 5px; display: inline-block;"> <p><b>[RESOLVED]</b> We are investigating a service degradation. This may impact your ability to perform tasks in the administrator</p> </div>

							console.
North America 2-03	✓	✓	✓	✓	✓	✓	✓
North America 2-04	✓	✓	✓	✓	✓	✓	✓

Page Last Updated: 6/19/2012 10:07:59 PM (UTC)

✓ Normal service availability	⚠ Service degradation	✗ Service interruption	✓ Additional information
-------------------------------	-----------------------	------------------------	--------------------------

## 9. SERVICE LEVELS

Microsoft offers a financially backed, 99.9 percent scheduled uptime Service Level Agreement (SLA) for the duration of the subscription term.

The 'Monthly Uptime Percentage' is calculated using the following formula:

$$\frac{\text{Total number of minutes in a month} \times \text{Total number of users} - \text{Total minutes of Downtime experienced by all users in that month}}{\text{Total number of minutes in a month} \times \text{Total number of users}}$$

## 10. FINANCIAL RECOMPENSE MODEL FOR NOT MEETING SERVICE LEVELS

Microsoft offers a financially backed, 99.9 percent scheduled uptime Service Level Agreement (SLA) for the duration of the subscription term. That means, if Microsoft does not meet the terms of the SLA the customer is eligible to receive service credits.

Standard Service Credits for Microsoft Online (Uptime Service Levels) are as follows:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

The full terms of service agreement for Windows Intune can be found in Appendix 1.

## 11. WINDOWS INTUNE TRAINING

There are several training resources for Windows Intune, please see below:

[Windows Intune TechCenter](#) - Get Started with the Springboard Series for Windows Intune

Proof of Concept (PoC) Days– Microsoft offer a number of PoC days, these are designed to provide a structured method to help customers understand the service and their current infrastructure readiness. Please contact the partner/account manager for further information

Ongoing Training - Ongoing training is also available from Certified Microsoft Partners.

Following is the Windows Intune Purchase, Provisioning and Technical support for general availability. If a customer is working with a Microsoft Partner or has questions regarding management services delivered by the partner, the customer should contact them first.

For questions regarding pre-purchase, purchase, provisioning, or activation, the customer can contact Microsoft Online Customer-Partner Care by calling one of the local numbers listed on [Microsoft Online Service Help and How to](#) or submit a support ticket [here](#).

### Technical Product Support

Online technical support is available by logging into the Windows Intune account and by clicking the Help link located at the top right-hand corner of the Windows Intune console (See image below). In addition, online and phone technical support is available [here](#).



## 12. TECHNICAL REQUIREMENTS

The technical requirements for Windows Intune are described below.

### Windows Intune Administrator Requirements

To use the Administrator Console, all that is required is a browser (IE7+) with Silverlight Installed and an internet Connection. Here is a list of the full Silverlight requirements <http://www.microsoft.com/getsilverlight/Get-Started/Install/Default.aspx>

### Client-side Requirements

#### PC Operating System Requirements

Windows Intune can now help you manage the entire family of Windows 8 devices, including:

1. Windows 8 Professional (x86 and x64 architectures).
2. Microsoft Surface Pro.
3. Microsoft Surface.
4. Windows RT devices.
5. Windows Phone 8 devices.

Windows Intune classifies Microsoft Surface, Windows RT, and Windows Phone 8 devices as mobile devices. Windows 8 and Microsoft Surface Pro devices are classified as fully managed PC devices, on which Windows Intune management and Endpoint Protection agents are installed. With the addition of these new clients, and the new capabilities of System Center Configuration Manager SP1, the management capabilities of the unified solution provides one of the most comprehensive range of clients supported in the industry. As a result, you'll be better equipped to manage the needs of a Bring Your Own Device (BYOD) infrastructure.

The Windows Intune client software is also supported on both 32-bit and 64-bit versions of:

- Windows 8 Professional
- Windows 7 Enterprise, Ultimate, and Professional
- Windows Vista Enterprise, Ultimate, and Business
- Windows XP Professional with Service Pack (SP) 3

The Windows Intune client software has no additional hardware requirements for computers running Windows 7 or Windows Vista. However, to install the client software on Windows XP-based computers, a CPU clock speed of 500 megahertz (MHz) or faster is needed and a minimum of 256 megabytes (MB) of RAM.

Administrator rights are required on the computer to complete the Windows Intune client software installation.

The Windows Intune Administration, Account and Company Portals are supported on the following web browsers: Microsoft Internet Explorer 8.0 and later, Google Chrome 19 and later, Mozilla Firefox 5 and later.

The Windows Intune Company Portal is also supported on web browsers for the following mobile device platforms: Microsoft Windows Phone 7.0 and later, Google Android 2.1 and later, Apple iOS 4.0 and later.

#### Client Components

When you enroll a client computer in the Windows Intune service, Windows Intune schedules the download and installation of additional agents, applications, and components to the client computer. These agents, applications, and components are updates to the initial Windows Intune client enrollment software package.

You can view the updates in the Windows Intune administrator console.

The following table describes the agents, applications, and components that are installed by Windows Intune.

Update name	Description
Update for Microsoft Online Management Components	This component helps Windows Intune update additional components that manage the client computer.
Windows Intune Endpoint Protection	These agents help protect the managed computer against potential threats by using real-time protection, automatic scans, and definition updates.
Windows Intune Monitoring Agent	These agents monitor the health of the managed computer, and raise alerts to report current and potential problems.
Microsoft Online Management Policy Agent	These agents let you configure settings on the managed computer and review information about software and hardware assets.
Update for Microsoft Online Management	This agent helps update the software on the managed computer.
Windows Intune Center	The Windows Intune Center allows users of the managed computer request remote assistance from administrators by using Remote Assistance via Microsoft Easy Assist v2, manage how some updates are deployed to the computer, and start scans for malware.
Windows Intune Notification Service	This agent helps deliver administrator-initiated commands to the managed computer.

 Note

For the correct operation of the managed computers, all the agent updates will be installed on the computers that are managed by Windows Intune. The updates apply to both the x86 and x64 architectures. When the agent updates are downloaded and installed, the status of this process is reported to Windows Intune. If any agent update is installed incorrectly, an alert is displayed in the Windows Intune administrator console.

**Supported Mobile Devices**

Windows Intune supports the following mobile and tablet devices:

- Windows Phone 7 or later
- iOS 4.0– and iOS 5.0–based devices or later
- Android-based phones and mobile devices 2.1 or later

Each of these mobile devices can now be managed with the Windows Intune service. Windows Intune uses Microsoft Exchange ActiveSync (EAS) to integrate management of users’ mobile devices with your infrastructure and to enforce your organization’s mobile device access policies. After the service is configured, it is possible to use

the Windows Intune administration console to manage both supported Windows-based computers and mobile devices.

### Scaling

Today, the Windows Intune administration experience is optimized for IT professionals looking to deliver the essentials of management and security for up to 5,000 PCs in a single account. The infrastructure is highly scalable, and as the service evolves, the usability of the administration console will continue to evolve to help IT professionals manage even larger enterprises.

For customers interested in managing more than 5,000 PCs, it is recommended to create multiple subscriptions of up to 5,000 PCs each.

Additionally, for customers who currently use the System Center configuration manager on-premises solution, there is a unified enterprise management solution. The Configuration Manager infrastructure enables support for very large installations. This release supports installations of up to approximately 100,000 users, computers, and mobile devices in a single management infrastructure. More information about this solution can be found here: <http://technet.microsoft.com/library/hh452635.aspx>.

### Firewall and Proxy Server Settings for Managed Computers

If there is a requirement to use Windows Intune to manage client computers that exist behind firewalls or proxy servers, the firewall or proxy server must be configured to allow Windows Intune to communicate with the client computers.

### Required firewall configuration

If the client computers exist behind a firewall, the firewall must be configured to allow communications with the domains through the specified ports that are listed in the following tables.

### Required domains for documentation, online Help, and support:

Domain	Ports
*.livemeeting.com	80 and 443
*.microsoftonline.com	80 and 443
onlinehelp.microsoft.com	80
*.social.technet.microsoft.com	80
blogs.technet.com	80
go.microsoft.com	80
<a href="http://www.microsoft.com">www.microsoft.com</a>	80

### Required domains for Microsoft Update Services:

Domain	Ports
*.update.microsoft.com	80 and 443
download.microsoft.com	80 and 443
update.microsoft.com	80 and 443

Depending on the firewall and how it processes DNS lookup requests, access to the domain manage.microsoft.com.nsatc.net on port 80 may be required.

### Required domains for Windows Intune and related services:

Domain	Ports
*.manage.microsoft.com	80 and 443
*manage.microsoft.com	80 and 443
*.spynet2.microsoft.com	443
manage.microsoft.com	80 and 443
wustat.microsoft.com	80 and 443
*manage.microsoft.com	80 and 443

### Required domains for Windows Update Services:

Domain	Ports
*.download.windowsupdate.com	80 and 443
*.windowsupdate.com	80 and 443
download.windowsupdate.com	80 and 443
ntservicepack.microsoft.com	80 and 443
windowsupdate.microsoft.com	80 and 443



## Required proxy server configuration

If the client computers exist behind a proxy server, the proxy server should be configured as follows:

Windows Intune communicates with client computers by using both the HTTP and HTTPS protocols. Confirm that the proxy server supports HTTP and HTTPS.

Windows Intune supports the Non-auth and Negotiate (Kerberos) authentication methods. If the proxy server uses the Negotiate (Kerberos) authentication method, the proxy server must allow computer accounts (instead of domain user accounts) to be enrolled in the service because the client software enrollment package runs as user LocalSystem.

The proxy server settings on individual client computers can be modified, or the Group Policy can be used to change settings for all client computers that exist behind a specified proxy server. Authenticated proxy servers are not supported.

## Bandwidth Optimization

To help ensure an optimal experience across the wide range of connection bandwidths available in different environments, Windows Intune now enables you to use the peer distribution platform in Windows 7 (Professional, Enterprise, Ultimate), which is one of the technologies that powers BranchCache.

Windows Intune has a policy setting that enables the limit for the network bandwidth to be specified, used by the Background Intelligent Transfer Service (BITS) during certain hours. By enabling this to use the peer distribution platform, this release of Windows Intune takes the ability to optimize network bandwidth to the next level. Software updates and applications can be transferred from a local subnet peer that has already downloaded it, which reduces the need to download content from the Internet.

In addition to saving Internet bandwidth, downloads from a local subnet peer provide increased download speed for your users who access the Windows Intune company portal to download available software applications. Windows Intune enables the peer distribution platform so that no server infrastructure is required; copies of files are directly cached on client computers on the network and sent to other client computers that run Windows 7 as needed. This feature can significantly reduce the network bandwidth required to deploy software applications and software updates, and the organization's Internet bandwidth usage.

## Windows Intune Content Caching

When updates and software distribution are managed from the Cloud, it is essential to minimize bandwidth load. Windows Intune addresses this requirement in two ways:

1. Using a caching web proxy server (such as Microsoft Forefront Threat Management Gateway (TMG) Server, Microsoft Internet Security and Acceleration (ISA) Server and SQUID Proxy Server) network bandwidth usage can be significantly reduced. Such caching web proxy servers can be configured to cache HTTP and updates binary download requests from Windows Intune to managed client computers. By avoiding duplicate downloads for content like Microsoft updates or endpoint protection signature updates, a caching web proxy server can significantly reduce the consumed Internet bandwidth.
2. Using Windows 7 Branch Cache to instrument client peer distribution.

## 13. DETAILS OF ANY TRIAL SERVICE AVAILABLE

Below are the following steps for a new customer wishing to get started with a free Windows Intune 30 day trial:

- 1) Customers goes to the [Windows Intune Homepage](#). - Select the "Try and Buy" tab.
- 2) Customer clicks the "Get the free 30 day trial now".
- 3) Customer creates a Windows Live ID or signs in using an existing Windows Live ID.

- 4) The customer completes the required fields to create their profile and sign up for your 30 day trial of Windows Intune. No Promotional Code is necessary. Note: The required "Subscription Identifier" field is a descriptor, such as the company name or general label that the customer would like to appear on your Windows Intune invoices should they choose to purchase the service upon completion of their trial in the future.
- 5) The customer will receive an email shortly after completing the registration. The customer can use the Windows Intune trial on up to 25 PCs [please note that the default is set to 25].

## **14. DATA EXTRACTION AND REMOVAL**

The method of facilitating data migration from Windows Intune to another Cloud-based service would be for the customer to run each of the following Windows Intune reports in full prior to their service shutdown:

- Update Report
- Detected Software Report
- Computer Inventory Report
- License Purchase Report
- License Installation Report
- Device Report
- User Information Report

This data is available for export in .csv and .html format. This can then be imported into their new solution.

## **15. DEPLOYMENT MODELS:**

Based on the definitions provided Windows Intune is a Public Cloud service.

## **APPENDIX 1 – MICROSOFT WINDOWS INTUNE SERVICE LEVEL AGREEMENT (SLA)**

THE SLA FOR VOLUME LICENSE CUSTOMERS IS LOCATED HERE:

[HTTP://WWW.MICROSOFTVOLUMELICENSING.COM/DOCUMENTSEARCH.ASPX?MODE=3&DOCUMENTTYPEID=37](http://www.microsoftvolumelicensing.com/documentsearch.aspx?mode=3&documenttypeid=37).

### **Service Level Agreement for Microsoft Online Services**

Last updated on: January 22, 2013

#### **1. Introduction.**

This Service Level Agreement for Microsoft Online Services (this “SLA”) is made by Microsoft in connection with, and is a part of, your Microsoft volume licensing agreement (the “Agreement”). This SLA applies to the following Microsoft Services:

- Bing Maps Professional
- Duet Enterprise Online
- Dynamics CRM Online
- Exchange Online Archiving
- Exchange Online
- Exchange Online Protection
- Lync Online
- Office Web Applications
- Project Online
- SharePoint Online
- Translator API
- Windows Azure Active Directory Rights Management
- Windows Intune
- Yammer Enterprise

We provide financial backing to our commitment to achieve and maintain the Service Levels for our Services. If we do not achieve and maintain the Service Levels for each Service as described in this SLA, then you may be eligible for a credit towards a portion of your monthly service fees. We will not modify the terms of your SLA during the initial term of your subscription; however, if you renew your subscription, then the version of this SLA that is current at the time of renewal will apply for your renewal term.

## 2. Definitions.

“Applicable Monthly Service Fees” means the total fees actually paid by you for a Service that are applied to the month in which a Service Credit is owed.

“Downtime” means the total minutes in a month during which the aspects of a Service specified in the following table are unavailable, excluding (i) Scheduled Downtime; and (ii) unavailability of a Service due to limitations described in Section 5(a) below.

Online Service	Qualifications of Downtime
Bing Maps Professional	Any period of time when the Service is not available as measured in Microsoft’s data centers, provided that you access the Service using the methods of access, authentication and tracking methods documented in the Bing Maps Platform SDKs.
Duet Enterprise Online	Any period of time when users are unable to read or write any portion of a SharePoint site collection for which they have appropriate permissions.
Dynamics CRM Online	Any period of time when end users are unable to read or write any Service data for which they have appropriate permission but this does not include non-availability of Service add-on features.
Exchange Online Archiving	Any period of time when end users are unable to access the e-mail messages stored in their archive.
Exchange Online	Any period of time when end users are unable to send or receive email with Outlook Web Access.
Exchange Online Protection	Any period of time when the network is not able to receive and process email messages.
Office Web Applications	Any period of time when users are unable to use the Web Applications to view and edit any Office document stored on a SharePoint site for which they have appropriate permissions.
Lync Online	Any period of time when end users are unable to see presence status, conduct instant messaging conversations, or initiate online meetings <sup>1</sup> .

Online Service	Qualifications of Downtime
Project Online	Any period of time when users are unable to read or write any portion of a SharePoint site collection with Project Web App for which they have appropriate permissions.
SharePoint Online	Any period of time when users are unable to read or write any portion of a SharePoint site collection for which they have appropriate permissions.
Translator API	Any period of time when users are not able to perform translations
Windows Azure Active Directory Rights Management	Any period of time when end users cannot create or consume IRM documents and email
Windows Intune	Any period of time when the Customer's IT administrator or users authorized by Customer are unable to log on with proper credentials.
Yammer Enterprise	Any period of time greater than ten minutes when more than five percent of end users are unable to post or read messages on any portion of the Yammer network for which they have appropriate permissions.

<sup>1</sup> Online meeting functionality applicable only to Lync Plan 2 Service

"Incident" means (i) any single event, or (ii) any set of events, that result in Downtime.

"Microsoft" means the Microsoft entity that entered into the Agreement.

"Scheduled Downtime" means periods of Downtime related to network, hardware, or Service maintenance or upgrades. We will publish notice or notify you at least five (5) days prior to the commencement of such Downtime.

"Service" or "Services" refers to the online service(s) indicated at the beginning of this SLA and purchased by you pursuant to the Agreement.

"Service Credit" is the percentage of the Applicable Monthly Service Fees credited to you following Microsoft's claim approval.

"Service Level" means the performance metric(s) set forth in this SLA that Microsoft agrees to meet in the delivery of the Services, e.g., monthly availability

3. **Service Level Commitment.** The "Monthly Uptime Percentage" for a Service is calculated by the following formula:

$$\frac{\text{Total number of minutes in a month} - \text{Downtime}}{\text{Total number of minutes in a month}} \times 100$$

---

If the Monthly Uptime Percentage falls below 99.9% for any given month, you may be eligible for the following Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

4. **Service Credit Claim.** If we fail to meet the minimum Monthly Uptime Percentage described above for a Service, you may submit a claim for a Service Credit.

You must submit a claim to customer support at Microsoft Corporation that includes: (i) a detailed description of the Incident; (ii) information regarding the duration of the Downtime; (iii) the number and location(s) of affected users (if applicable); and (iv) descriptions of your attempts to resolve the Incident at the time of occurrence. We must receive the claim and all required information by the end of the calendar month following the month in which the Incident occurred. For example, if the Incident occurred on February 15<sup>th</sup>, we must receive the claim and all required information by March 31<sup>st</sup>.

We will evaluate all information reasonably available to us and make a good faith judgment on whether a Service Credit is owed. We will use commercially reasonable efforts to process claims during the subsequent month and within forty five (45) days of receipt. You must be in compliance with the Agreement in order to be eligible for a Service Credit. If we determine that a Service Credit is owed to you, we will apply the Service Credit to your Applicable Monthly Service Fees.

If you purchased a Service from a reseller, you will receive a service credit directly from your reseller and the reseller will receive a Service Credit directly from us.

## 5. **Limitations.**

- (a) This SLA and any applicable Service Levels do not apply to any performance or availability issues:

1. Due to factors outside our control;
2. That result from your or third party services, hardware, or software;
3. Caused by your use of a Service after we advised you to modify your use of a Service, if you did not modify your use as advised;
4. During pre-release, beta and trial Services (as determined by us);
5. That result from your unauthorized action or inaction or from your employees, agents, contractors, or vendors, or anyone gaining access to our network by means of your passwords or equipment; or
6. That result from your failure to adhere to any required configurations, use supported platforms, and follow any policies for acceptable use.
7. For licenses reserved, but not paid for, at the time of the Incident.

- (b) Service Credits are your sole and exclusive remedy for any performance or availability issues for any Service under the Agreement and this SLA. You may not unilaterally offset your Applicable Monthly Service Fees for any performance or availability issues.

- (c) This SLA will not apply to any on-premise licensed software that is part of any Service.

- 
- 6. Purchase of Multiple Services.** If you purchased more than one Service listed in Section 1 above (not as a suite), then you may submit claims pursuant to the process described above in Section 4 as if each Service was covered by an individual SLA. For example, if you purchased both Exchange Online and SharePoint Online (not as part of a suite), and during the term of the subscription an Incident caused Downtime for both Services, then you could be eligible for two separate Service Credits (one for each Service), by submitting two claims under this SLA.
- 7. Purchase of Multiple Services together.** If you purchased Services as part of a suite or other single offer, the Applicable Monthly Service Fees and Service Credit for each Service will be prorated.
- 8. Exceptions and Additional Terms for Particular Services and Programs.**

**(a) For Bing Maps Professional:**

This SLA does not apply to Bing Maps Professional purchased through Open Value and Open Value Subscription licensing agreements.

Service Credits will not apply if: (i) you fail to implement any Services updates within the time specified in the Bing Maps Platform API's Terms of Use; and (ii) you do not provide Microsoft with at least ninety (90) days' advance notice of any known significant usage volume increase, with significant usage volume increase defined as 50% or more of the previous month's usage.

**(b) For Duet Enterprise Online:**

You will be eligible for a Service Credit for Duet Enterprise Online only when you are eligible for a Service Credit for the SharePoint Online Plan 2 User SLs that you have purchased as a prerequisite for your Duet Enterprise Online User SLs. This SLA does not apply when the inability to read or write any portion of a SharePoint site is caused by any failure of third party software, equipment, or services that are not controlled by Microsoft, or Microsoft software that is not being run by Microsoft itself as part of the Service.

**(c) For Exchange Online, Exchange Online Archiving (EOA), and Exchange Online Protection (EOP):**

There is no Scheduled Downtime for these Services.

**(d) For Exchange Online and Exchange Online Protection (EOP):**

With respect to Exchange Online and EOP licensed as a standalone Service or via ECAL suite, or Exchange Enterprise CAL with Services, you may be eligible for Service Credits if we do not meet the Service Level described below for: (1) Virus Detection and Blocking, (2) Spam Effectiveness, or (3) False Positive. If any one of these individual Service Levels is not met, you may submit a claim for a Service Credit. If one Incident causes us to fail more than one SLA metric for Exchange Online or EOP, you may only make one Service Credit claim for that incident per Service.

1. Virus Detection and Blocking Service Level

- a. "Virus Detection and Blocking" is defined as the detection and blocking of Viruses by the filters to prevent infection. "Viruses" is broadly defined as known malware, which includes viruses, worms, and Trojan horses. For classification of malware, please visit

[http://www.microsoft.com/technet/security/topics/serversecurity/avdind\\_2.msp](http://www.microsoft.com/technet/security/topics/serversecurity/avdind_2.msp)

- b. A Virus is considered known when a EOP virus scanning engine can detect the virus and the detection capability is available throughout the EOP network.
- c. Must result from a non-purposeful infection.
- d. The Virus must have been scanned by the EOP virus filter.
- e. If EOP delivers an email that is infected with a known virus to you, EOP will notify you and work with you to identify and remove the virus. If this results in the prevention of an infection, you will not be eligible for a Service Credit under the Virus Detection and Blocking Service Level.
- f. The Virus Detection and Blocking Service Level shall not apply to:
  - 1. Forms of email abuse not classified as malware, such as spam, phishing and other scams, adware, and spyware. For classification of malware, please visit [http://www.microsoft.com/technet/security/topics/serversecurity/avdind\\_2.msp](http://www.microsoft.com/technet/security/topics/serversecurity/avdind_2.msp).
  - 2. Corrupt, defective, truncated, or inactive viruses contained in NDRs, notifications, or bounced emails.
- g. The Service Credit available for the Virus Detection and Blocking Service is: 25% Service Credit of Applicable Monthly Service Fee if an infection occurs in a calendar month, with a maximum of one claim allowed per calendar month.

2. Spam Effectiveness Service Level

- a. "Spam Effectiveness" is defined as the percentage of inbound spam detected by the filtering system, measured on a daily basis.
- b. Spam effectiveness estimates exclude false negatives to invalid mailboxes.
- c. The spam message must be processed by our service and not be corrupt, malformed, or truncated.
- d. The Spam Effectiveness Service Level does not apply to email containing a majority of non-English content.
- e. You acknowledge that classification of spam is subjective and accept that we will make a good faith estimation of the spam capture rate based on evidence timely supplied by you.
- f. The Service Credit available for the Spam Effectiveness Service is:

% of Calendar Month that Spam Effectiveness is below 98%	Service Credit
> 25%	25%
> 50%	50%
100%	100%

3. False Positive Service Level

- a. "False Positive" is defined as the ratio of legitimate business email incorrectly identified as spam by the filtering system to all email processed by the service in a calendar month.
- b. Complete, original messages, including all headers, must be reported to the abuse team.
- c. Applies to email sent to valid mailboxes only.
- d. You acknowledge that classification of false positives is subjective and understand that we will make a good faith estimation of the false positive ratio based on evidence timely supplied by you.



- e. This False Positive Service Level shall not apply to:
1. bulk, personal, or pornographic email
  2. email containing a majority of non-English content
  3. email blocked by a policy rule, reputation filtering, or SMTP connection filtering
  4. email delivered to the junk folder
- f. The Service Credit available for the False Positive Service is:

False Positive Ratio in a Calendar Month	Service Credit
> 1:250,000	25%
> 1:10,000	50%
> 1:100	100%

**(e) For Exchange Online Archiving (EOA) and Exchange Online Protection (EOP):**

This SLA does not apply to the Enterprise CAL suite purchased through Open Value and Open Value Subscription licensing agreements.

**(f) For Exchange Online Protection (EOP):**

With respect to EOP licensed as a standalone Service, ECAL suite, or Exchange Enterprise CAL with Services, you may be eligible for Service Credits if we do not meet the Service Level described below for (1) Uptime and (2) Email Delivery.

1. Monthly Uptime Percentage:

If the Monthly Uptime Percentage for EOP falls below 99.999% for any given month, you may be eligible for the following Service Credit:

Monthly Uptime Percentage	Service Credit
<99.999%	25%
<99.0%	50%
<98.0%	100%

2. Email Delivery Service Level:

- a. "Email Delivery Time" is defined as the average of email delivery times, measured in minutes over a calendar month, where email delivery is defined as the elapsed time from when a business email enters the EOP network to when the first delivery attempt is made.
- b. Email Delivery Time is measured and recorded every 5 minutes, then sorted by elapsed time. The fastest 95% of measurements are used to create the average for the calendar month.
- c. We use simulated or test emails to measure delivery time.

- d. The Email Delivery Service Level applies only to legitimate business email (non-bulk email) delivered to valid email accounts.
- e. This Email Delivery Service Level does not apply to:
  1. Delivery of email to quarantine or archive
  2. Email in deferral queues
  3. Denial of service attacks (DoS)
  4. Email loops
- f. The Service Credit available for the Email Delivery Service is:

Average Email Delivery Time (as defined above)	Service Credit
> 1	25%
> 4	50%
> 10	100%

**(g) For Windows Azure Active Directory Rights Management:**

There is no Scheduled Downtime for this Service.

**(h) For Windows Intune:**

1. Scheduled Downtime will not exceed 10 hours per calendar year
2. This Service Level does not apply to any:
  - a. On-premises software licensed as part of the Service subscription.
  - b. Internet-based services (excluding the Windows Intune Service) that provide updates to any on-premise software licensed as part of the Service subscription.

**(i) This section (i) applies to the following:**

- Each of the Services in Office 365 Midsize Business suite purchased through Open, Open Value and Open Value Subscription licensing agreements,
- Exchange Online Archiving (EOA) purchased through Open Value and Open Value Subscription licensing agreements, and
- Each of the Services in Office 365 Small Business Premium suite purchased in the form of a product key

These Services are not eligible for Service Credits based on service fees. Any Service Credit that you may be eligible for will be credited in the form of service time (i.e., days) as opposed to service fees.

For these Services,

1. the definition of “Applicable Monthly Service Fees” shall be deleted and replaced by: “Applicable Monthly Period” means, for a calendar month in which a Service Credit is owed, the number of days that you are a subscriber for a Service.

- 
2. Any references to “Applicable Monthly Service Fees” shall be deleted and replaced by “Applicable Monthly Period.”