FIREBRAND

MCSA Windows Client
Windows 8.1

SUPPLEMENTAL TRAINING MATERIAL FOR EXAM70-688

FIREBRAND TRAINING

www.firebrandtraining.com

Contents

Courseware Overview

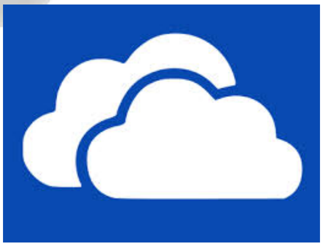
This supplemental material is designed to complement the Microsoft Official Courseware used on the course.

During the 70-687 MOC you were introduced to several Microsoft technologies which are used to support, enhance and control the Windows 8.1 desktop environment. Most of these technologies are also backwards compatible with older operating systems (Windows 7 / Windows 8).

Delegates should note that these are constantly changing technologies which are evolving with the development of System Center and Cloud-based products and therefore all references within this document are subject to change. Your course instructor will advise you of any significant changes as they occur.

Microsoft Technet references are given throughout and are suitable links for further information.

Microsoft OneDrive



Microsoft OneDrive (formerly SkyDrive) is free cloud storage that comes with your Microsoft account. OneDrive is built into Windows 8.1 and Windows 8.1 Tablets by default, giving the user an allocation of free storage (currently up to 10Gb).

OneDrive for Business (formerly SkyDrive Pro) allows for a single user within the enterprise to synchronise and store files and folders from Office 365/Sharepoint applications across the cloud.

OneDrive represents a fairly easy and flexible storage solution for all types of users. Home and Small business users may enable synchronisation of documents, photos, videos between desktop and mobile devices. Windows Phone and Tablet devices enable automatic synchronisation between pictures and the Camera Roll folder over non metered connections.

Office 365

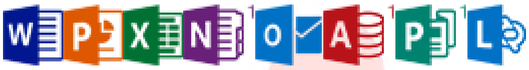
Microsoft Office 365 provide a Software as a Service (SaaS) platform for both Home and Business users.

A variety of plans are available in accordance with the size of the corporation ranging from Small Business to Enterprise solutions.

Depending upon your subscription – several key Microsoft products are available:

These include: (As taken from the Microsoft Office 365 Website)

The latest versions of Microsoft Office suite:



Office on more devices	Enjoy a consistent and familiar Office experience across PCs, Macs, Windows tablets, and most mobile devices.
Office on any PC	Stream full versions of Office programs on any Internet-connected PC running Windows 7 or Windows 8 with Office on Demand.

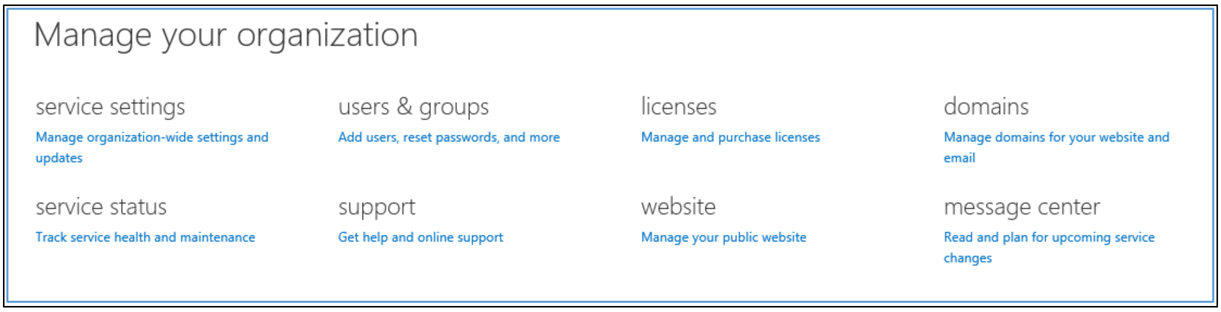
- Plus these online services:

Email and calendars	Use business-class email through a rich and familiar Outlook experience you can access from your desktop or from a web browser using Outlook Web App. Get a 50 GB mailbox per user and send attachments up to 25 MB.
Simple file sharing	SkyDrive Pro provides 25 GB of storage for each user for virtually anywhere access to their documents. Share files with others inside and outside the organization, control who can see and edit each file, and easily sync files with PCs and devices.
Public website	Design and maintain your own public website with no additional hosting fees. Use your own domain name to promote your brand.
Team sites	Enable easy access and sharing of documents with 10 GB baseline storage plus 500 MB of storage per user.
Web conferencing	Host online meetings with audio and video using one-click screen sharing and HD video conferencing.
Instant messaging and Skype connectivity	Connect with other Lync users via instant message, voice calls, and video calls, and let people know your availability with your online status. Share presence, IM, and audio calling with Skype users.

Office Mobile Apps	Stay productive and never miss a meeting, even on the go. Access, edit, and view Word, Excel, and PowerPoint documents on iPhones, Android phones, and Windows Phones. Use the OneNote, Lync Mobile, and SharePoint Newsfeed apps on most devices.
Reliability	Get peace of mind knowing your services are available with a a guaranteed 99.9% uptime, financially backed service level agreement (SLA).
Security	Your data is yours. We safeguard it and protect your privacy.
Administration	Deploy and manage Office 365 across your company, no IT expertise required. You can add and remove users in minutes.
Support	Microsoft Support provides telephone and online answers, how-to resources, and connections with other Office 365 customers for setup and quick fixes.

Office 365 does constitute a relatively easy to set up solution for small and large business who predominantly use Microsoft productivity products. It also offers a flexible pricing scheme and works alongside a range of other Microsoft Cloud-based technologies.

Office 365 Administration Dashboard:



Manage your organization

service settings
Manage organization-wide settings and updates

users & groups
Add users, reset passwords, and more

licenses
Manage and purchase licenses

domains
Manage domains for your website and email

service status
Track service health and maintenance

support
Get help and online support

website
Manage your public website

message center
Read and plan for upcoming service changes

http://technet.microsoft.com/en-us/library/hh852466(v=technet.10)

Active Sync

Microsoft Active Sync is a technology which was introduced with Windows 95 however the latest version of software is compatible with Windows XP SP2 and above. Active Sync is available in two ways:

- Microsoft Active Sync – used to synchronise data between mobile devices
- Exchange Active Sync – used to push email, contacts and calendar events to recipients from Exchange Server or Office 365 Server.

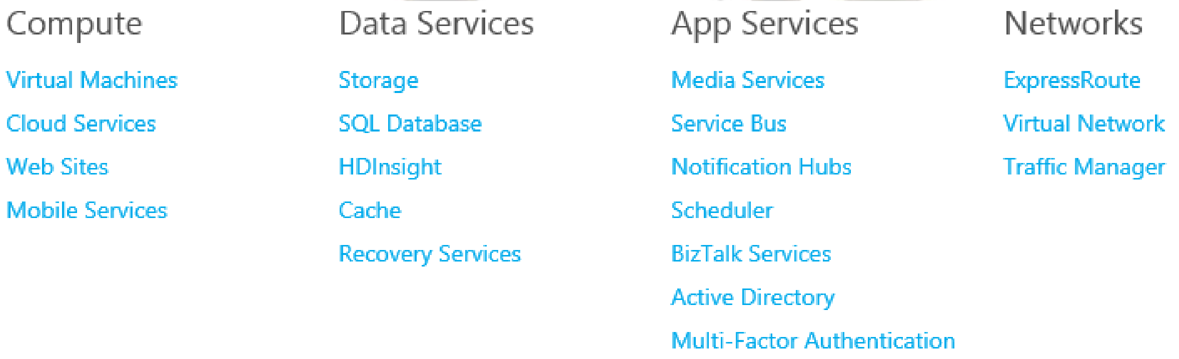
Both technologies are predominantly focused on supporting Windows devices but may be used on Android and Apple devices.

Setup is relatively straight forward (and wizard driven on most Windows devices) and uses POP/IMAP and SMTP connections in accordance with your email services.

http://technet.microsoft.com/en-us/library/aa998357(v=exchg.150).aspx

Microsoft Azure

Microsoft Azure provides a full Cloud solution offering a pay as you use service for IaaS, Paas and SaaS technologies with an SLA maintaining 99.95% up time. The component parts of Azure are broken down as:



Compute

- Virtual Machines
- Cloud Services
- Web Sites
- Mobile Services

Data Services

- Storage
- SQL Database
- HDInsight
- Cache
- Recovery Services

App Services

- Media Services
- Service Bus
- Notification Hubs
- Scheduler
- BizTalk Services
- Active Directory
- Multi-Factor Authentication

Networks

- ExpressRoute
- Virtual Network
- Traffic Manager

What is Windows Azure Active Directory?

Windows Azure Active Directory is a service that provides identity and access management capabilities in the cloud. In much the same way that Active Directory is a service made available to customers through the Windows Server operating system for on-premises identity management, Windows Azure Active Directory (Windows Azure AD) is a service that is made available through Windows Azure for cloud-based identity management because it is your organization's cloud directory, you decide who your users are, what information to keep in the cloud, who can use the information or manage it, and what applications or services are allowed to access that information.

When you use Windows Azure AD, it is Microsoft's responsibility to keep Active Directory running in the cloud with high scale, high availability, and integrated disaster recovery, while fully respecting your requirements for the privacy and security of your organization's information.

Integration with your on-premises Active Directory

Windows Azure AD can be used as a standalone cloud directory for your organization, but you can also integrate existing on-premise Active Directory with Windows Azure AD. Some of the features of integration include directory sync and single sign-on, which further extend the reach of your existing on-premises identities into the cloud for an improved admin and end user experience.

Integration with your applications

Application developers can integrate their applications with Windows Azure AD to provide single sign-on functionality for their users. This enables enterprise applications to be hosted in the cloud and to easily authenticate users with corporate credentials. It also enables software as a service (SaaS) providers to make authentication easier for users in Windows Azure AD organizations when authenticating to their services.

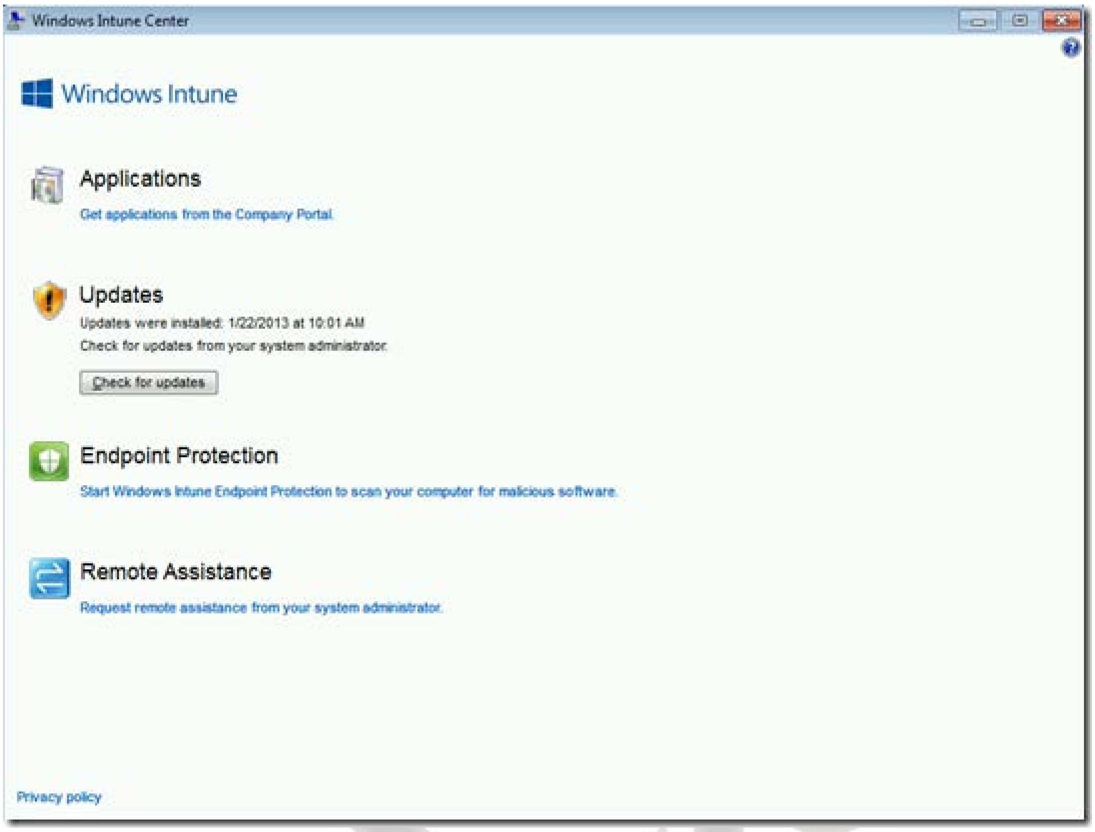
https://www.windowsazure.com/en-us/documentation/

Windows Intune

Windows Intune is an integrated, cloud-based client management solution that provides tools, reports, and upgrade licenses to the latest version of Windows. Windows Intune helps keep your computers up-to-date and secure. It also allows you to manage mobile devices on your network either through Exchange ActiveSync or directly through Windows Intune while providing versatile management capabilities for iOS, Android, Windows RT and Windows Phone 8 devices.

The following topics describe the management tasks that you can perform by using the workspaces in the Windows Intune administrator console. They also describe how you can use the Windows Intune account portal to manage the business account for the Windows Intune service and to control which users are managed by Windows Intune. In addition, these topics describe the Windows Intune company portal, which lets your users more securely access and install available licensed software applications and perform other common tasks without the need for IT staff assistance.

Windows Intune supports Windows 7 and Windows 8 clients however at the time of writing full functionality is not available with Windows 8 and 8.1 clients. Remote assistance is currently only available for Windows 7 Clients.



Windows Intune

Applications

Get applications from the Company Portal

Updates

Updates were installed: 1/22/2013 at 10:01 AM

Check for updates from your system administrator.

Endpoint Protection

Start Windows Intune Endpoint Protection to scan your computer for malicious software.

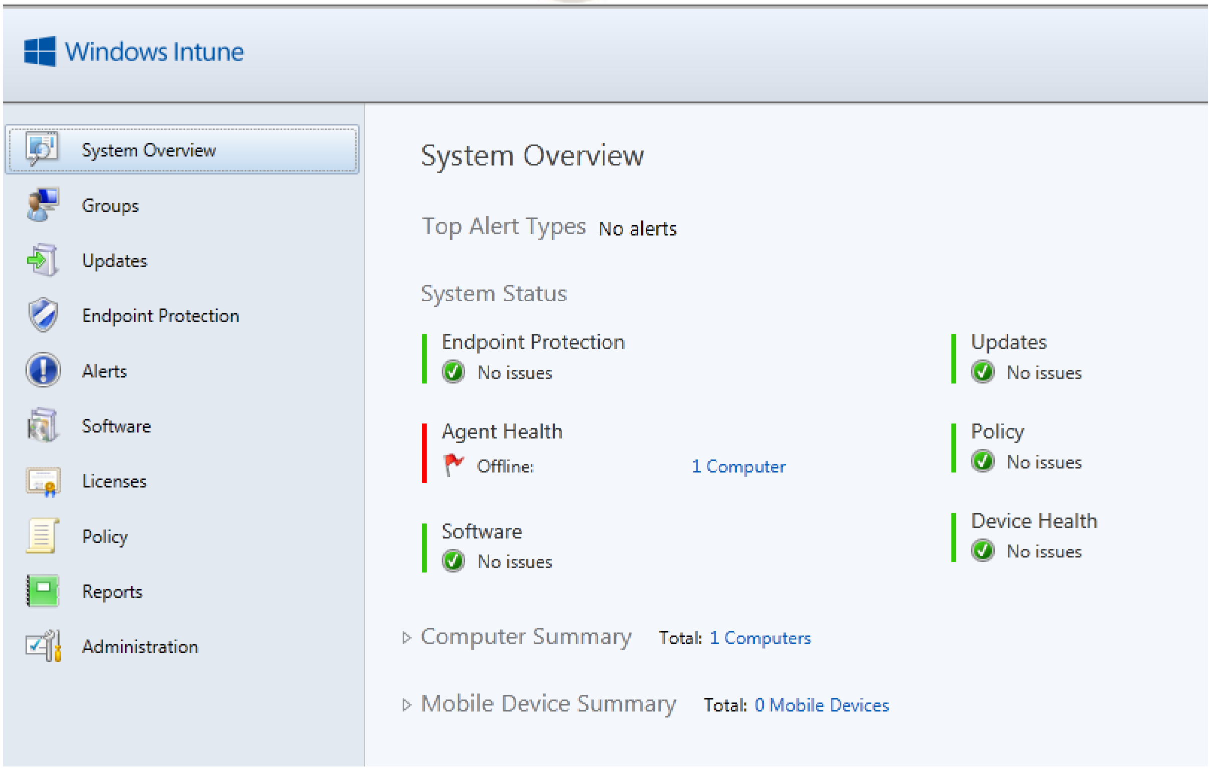
Remote Assistance

Request remote assistance from your system administrator.

Privacy policy

Windows Intune Center for Windows 8 (Remote Assistance currently unavailable)

Windows Intune - Administration



Windows Intune

System Overview

Top Alert Types No alerts

System Status

Endpoint Protection
✓ No issues

Updates
✓ No issues

Agent Health
Offline: 1 Computer

Policy
✓ No issues

Software
✓ No issues

Device Health
✓ No issues

▷ Computer Summary Total: 1 Computers

▷ Mobile Device Summary Total: 0 Mobile Devices

- **Windows Intune Account Portal**

The Windows Intune account portal lets you manage your Windows Intune subscription and specify the users who can access Windows Intune. From the account portal, you can perform tasks such as manually adding user accounts and security groups, setting up and managing service settings, checking service status, and accessing online help. You can also access the Windows Intune administrator console and the Windows Intune company portal. Users can access the account portal to change their password.

- **Windows Intune Groups**

Windows Intune provides you with a great deal of flexibility for managing your devices and users by organizing them into groups. You can organize groups in the way that best suits your organizational needs (for example, by geographic location, department, or hardware characteristics). A device or a user can belong to more than one group.

Groups in Windows Intune can now have dynamic membership queries or rules, static membership, or mixed membership. When you create a dynamic membership query, you define the criteria that determines the query that Windows Intune runs to retrieve the list of group members. The group is automatically updated with members that meet the criteria whenever changes occur. You can also create groups that have static membership lists. These are groups that you manually define by explicitly adding members

- **The Updates Workspace**

In Windows Intune, you can use the Updates workspace to administer the software update process efficiently for all the managed computers in your organization. The Windows Intune administrator console supports and encourages best practices for update management so that you can focus on your environment and the tasks that you have to perform. The Updates workspace in the Windows Intune administrator console provides you with quick access to tasks, so that you can view pending updates, approve or decline updates, configure automatic approval settings, and set a deadline for update installation in an automatic approval rule.

You can approve and deploy Microsoft and non-Microsoft updates. To deploy non-Microsoft updates, you create the update software packages and then upload them to the Windows Intune Cloud Storage space. After you upload the updates, they are displayed in the Updates workspace and you can approve and deploy them to managed computers.

As updates are approved and installed, the update status changes to reflect the success or failure of the installation.

- **Endpoint Protection**

Windows Intune Endpoint Protection helps enhance the security of computers in your organization by providing real-time protection against potential threats, keeping malicious software definitions up to date, and automatically running scheduled scans. The Windows

Intune Endpoint Protection workspace in the Windows Intune administrator console provides Endpoint Protection status summaries so that if malicious software is detected on a managed computer, or if a computer is not protected, you can quickly identify the affected computers and take appropriate action. You can also configure alert notification rules to notify you or others by email of a detected threat.

You can schedule automatic scans by using Policy, and at any time you can also run a remote task to initiate a quick scan or a full scan, or update malware definitions on a computer

A quick scan checks the places, processes in the memory, and registry files on the hard disk that malicious software, or malware, is most likely to infect. A full scan checks all files on the hard disk and all currently running programs, so a full scan could cause managed computers to run slowly until the scan is complete. By default, quick scans are scheduled daily at 2 A.M. on computers that are not being used. Also by default, Windows Intune checks for the latest virus and spyware definitions before quick scans are run.

Links on the Endpoint Protection Overview page in the console connect you to relevant Microsoft Malware Protection Center topics where you can learn more about malicious software that might be affecting computers in your organization.

- **The Software Workspace**

In the Windows Intune™ administrator console, the Software workspace lists the detected and managed software that is installed on all computers that you are managing by using Windows Intune. Software inventory is only available for computers, not mobile devices. You can sort the detected or the managed software inventory by clicking the column headings in either list. Each unique software title has its own entry in the list, and you can also search for a specific software title in both lists, and filter the managed software list.

From the Software workspace, you can deploy a managed software package, or a link to a web-based application or an application in the Windows Store for the Windows, Windows RT, Windows Phone 8, iOS, and Android platforms. For Windows-based software, you can configure a Required Install deployment to be automatically installed on targeted managed computers without the need for end-user intervention. You can also make a licensed software application available from the Windows Intune company portal for approved end users to link to, or download, and install on their linked computers or applicable mobile devices

- **The Policy Workspace**

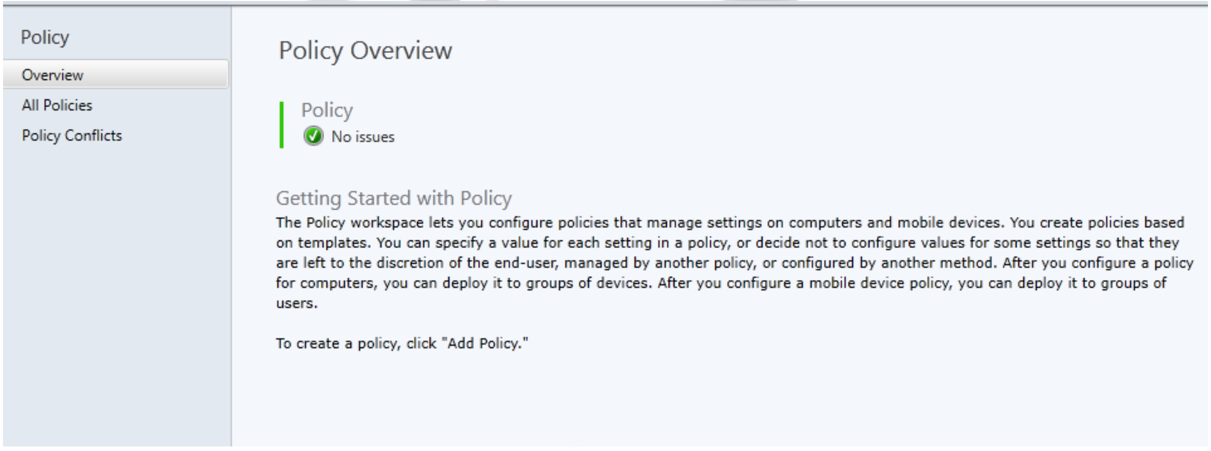
Windows Intune policies provide settings that control software updates, Endpoint Protection, Windows Firewall settings, and the end-user experience in the Windows Intune Center, which is installed on all computers that are managed by Windows Intune. Windows Intune also provides settings to control the security of users’ mobile devices, including Windows RT, Windows Phone 8, and Apple iOS devices. In the Windows Intune administrator console, you can use the Policy workspace to create policies based on templates, configure policy settings, and then deploy policies to device or user groups.

Policy templates also now include the option to deploy policies with recommended settings, so that you can easily create and deploy policies that implement best practices. In addition, Windows Intune provides detailed information about mobile policy conflicts and recommended actions to take, so that you can quickly identify conflicting mobile policy settings, and then resolve the conflicts. You can also force a refresh on policies on computers by using the Refresh Policies remote task.

In the Policy workspace, a status summary lets you quickly identify and prioritize issues that require your immediate attention. You can also search for policies by name or description. A policy status summary also appears on the System Overview page.

See below for a full break down of InTune Policies.

Policy Overview



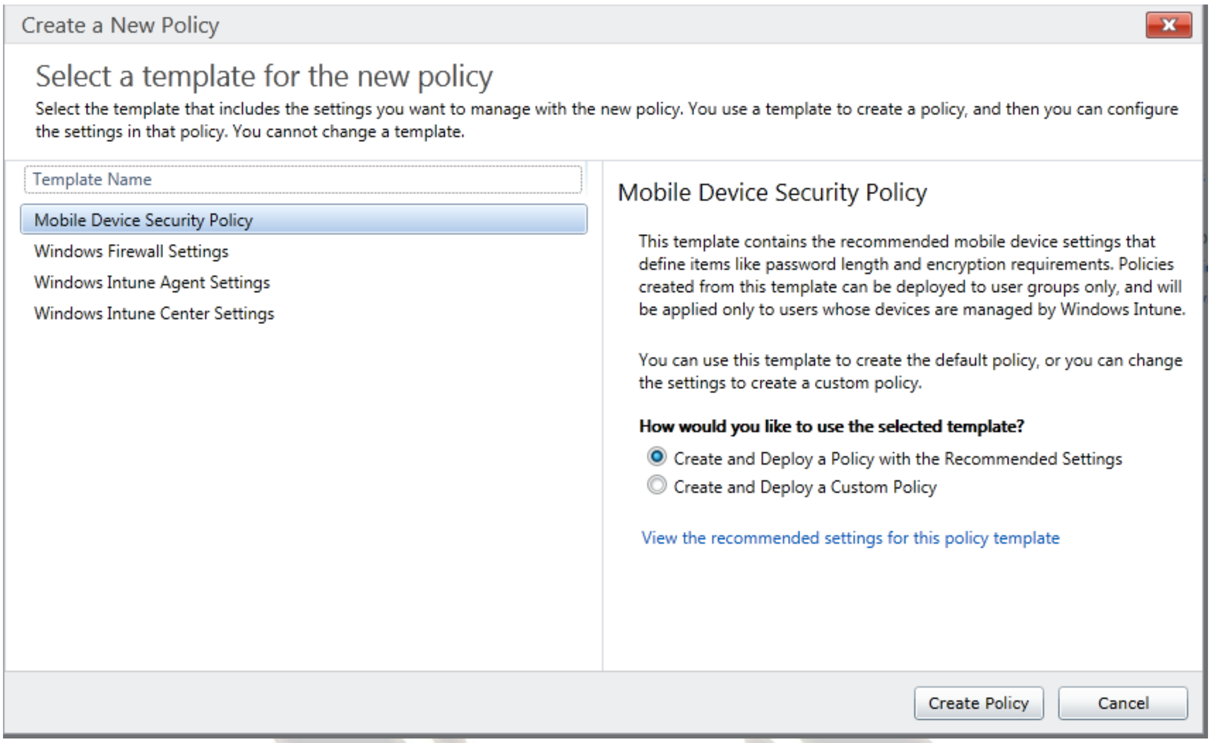
Policy Overview

Policy
✓ No issues

Getting Started with Policy

The Policy workspace lets you configure policies that manage settings on computers and mobile devices. You create policies based on templates. You can specify a value for each setting in a policy, or decide not to configure values for some settings so that they are left to the discretion of the end-user, managed by another policy, or configured by another method. After you configure a policy for computers, you can deploy it to groups of devices. After you configure a mobile device policy, you can deploy it to groups of users.

To create a policy, click "Add Policy."



Create a New Policy

Select a template for the new policy

Select the template that includes the settings you want to manage with the new policy. You use a template to create a policy, and then you can configure the settings in that policy. You cannot change a template.

Template Name
Mobile Device Security Policy
Windows Firewall Settings
Windows Intune Agent Settings
Windows Intune Center Settings

Mobile Device Security Policy

This template contains the recommended mobile device settings that define items like password length and encryption requirements. Policies created from this template can be deployed to user groups only, and will be applied only to users whose devices are managed by Windows Intune.

You can use this template to create the default policy, or you can change the settings to create a custom policy.

How would you like to use the selected template?

● Create and Deploy a Policy with the Recommended Settings
○ Create and Deploy a Custom Policy

View the recommended settings for this policy template

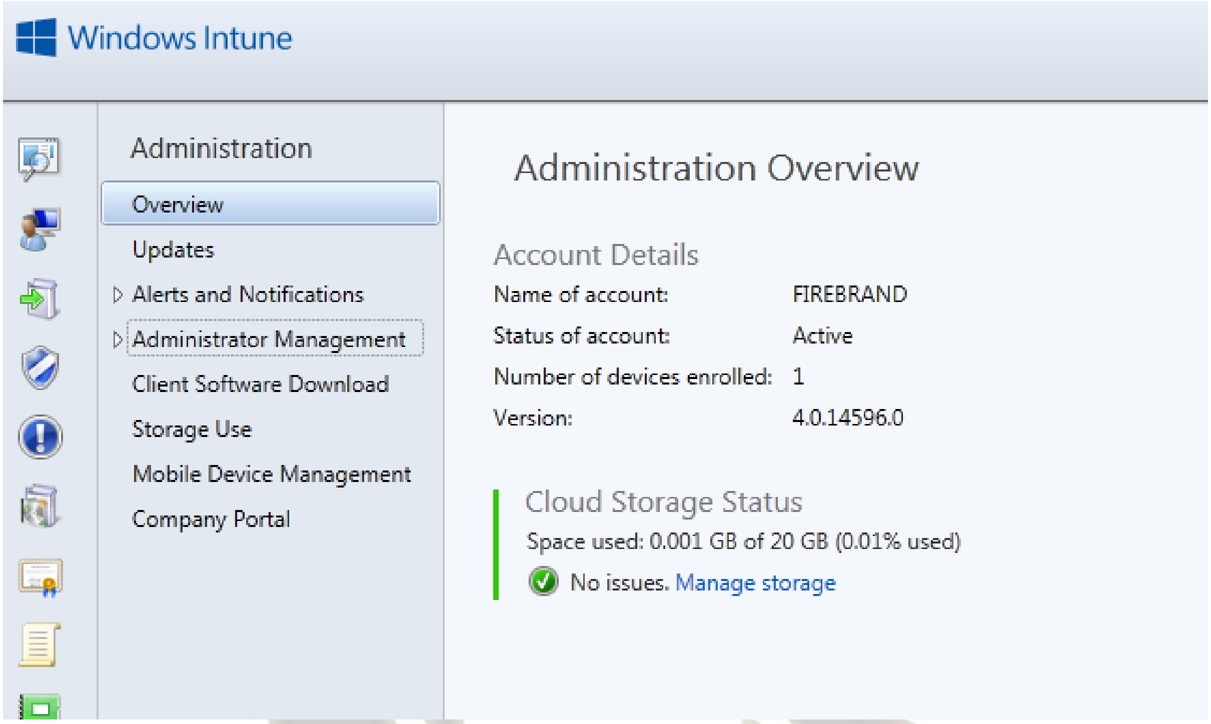
The Four Intune Policies are:

Mobile Device Security Policy: Enables the administrator to define Mobile device settings such as Password lengths and encryption, lockout thresholds and unlock methods, malware settings, application and device capabilities.

Windows Firewall Settings: Enables the administrator to turn on and configure Firewall Profiles (Domain, Private and Public) including exceptions for incoming/outgoing rules for applications.

Windows Intune Agent Settings: Policy which controls the deployment of the Intune Agent and Endpoint Protection onto clients.

Windows Intune Center Settings: Policy which defines the contents and deployment of the Intune Center Settings, such as responsible administrator, contact details etc.



Administration Overview

Account Details

Name of account:	FIREBRAND
Status of account:	Active
Number of devices enrolled:	1
Version:	4.0.14596.0

Cloud Storage Status

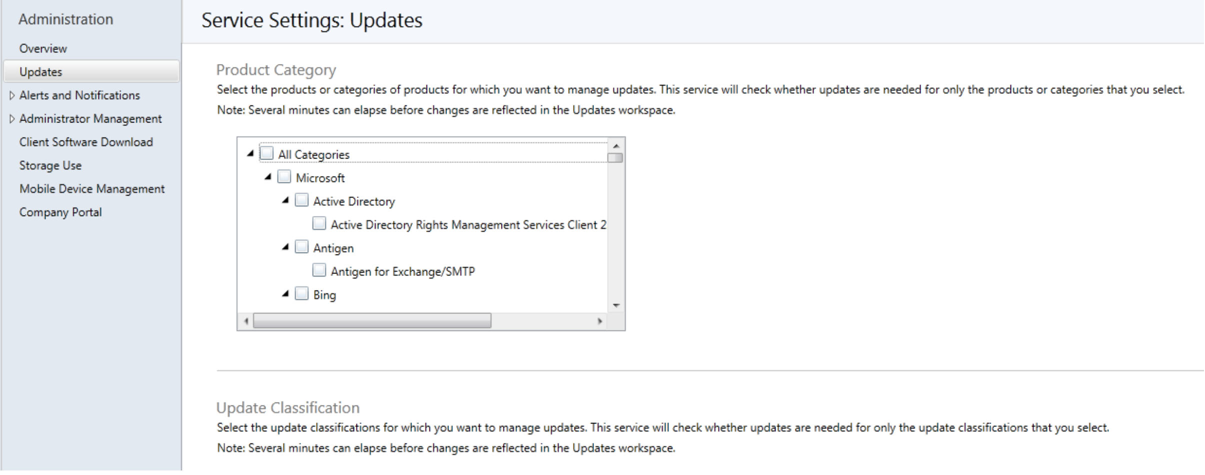
Space used: 0.001 GB of 20 GB (0.01% used)

✓ No issues. Manage storage

- **Administration**

In the Windows Intune™ administrator console, in the Administration workspace, you can view details about your Windows Intune account (such as account name, status, and active seat count) and perform the following tasks:

• Updates: Configure service settings to select the products or categories of products for which you want to manage updates, and the update classifications for which you want to manage updates. When you do this, Windows Intune checks whether updates are needed for only the products or categories and update classifications that you select. To ensure that all critical and security updates are installed as quickly as possible on your managed computers, you can also set up automatic update approval rules and deadlines for installation of approved updates.



Service Settings: Updates

Product Category

Select the products or categories of products for which you want to manage updates. This service will check whether updates are needed for only the products or categories that you select.

Note: Several minutes can elapse before changes are reflected in the Updates workspace.

- □ All Categories
  - □ Microsoft
    - □ Active Directory
      - □ Active Directory Rights Management Services Client 2
    - □ Antigen
      - □ Antigen for Exchange/SMTP
    - □ Bing

Update Classification

Select the update classifications for which you want to manage updates. This service will check whether updates are needed for only the update classifications that you select.

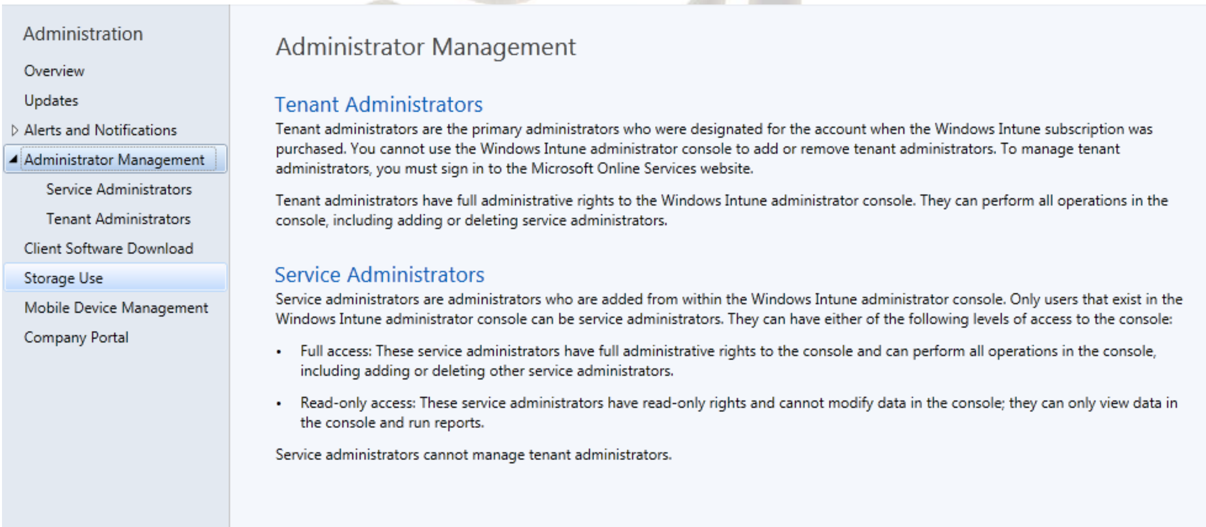
Note: Several minutes can elapse before changes are reflected in the Updates workspace.

- Alerts and Notifications: Enable alert types that are important, disable those that are not important, and set Monitoring alert thresholds for alert types so that Windows Intune can notify you if a threshold was met or exceeded. You can also configure Windows Intune to send you or other users email notifications about new alerts, based on rules that you set

- Administrator Management: Designate Windows Intune service administrators who have either full access or read-only access to the Windows Intune administrator console.

You can also view the list of Windows Intune tenant administrators. **Tenant administrators have full administrative rights to the Windows Intune administrator console**. They can perform all operations in the console, including adding or deleting Windows Intune service administrators. In addition, they can assign other tenant administrators by using the Windows Intune account portal. To add, delete, or manage tenant administrators, you must sign in to the Windows Intune account portal.

By default, the individual who subscribes to Windows Intune becomes a global administrator for Microsoft Online Services and a tenant administrator for the Windows Intune administrator console. As a global administrator for Microsoft Online Services, that individual has the same privileges across all Microsoft Online Services for the organization and can add other tenant administrators for the Windows Intune administrator console.



Administrator Management

Tenant Administrators

Tenant administrators are the primary administrators who were designated for the account when the Windows Intune subscription was purchased. You cannot use the Windows Intune administrator console to add or remove tenant administrators. To manage tenant administrators, you must sign in to the Microsoft Online Services website.

Tenant administrators have full administrative rights to the Windows Intune administrator console. They can perform all operations in the console, including adding or deleting service administrators.

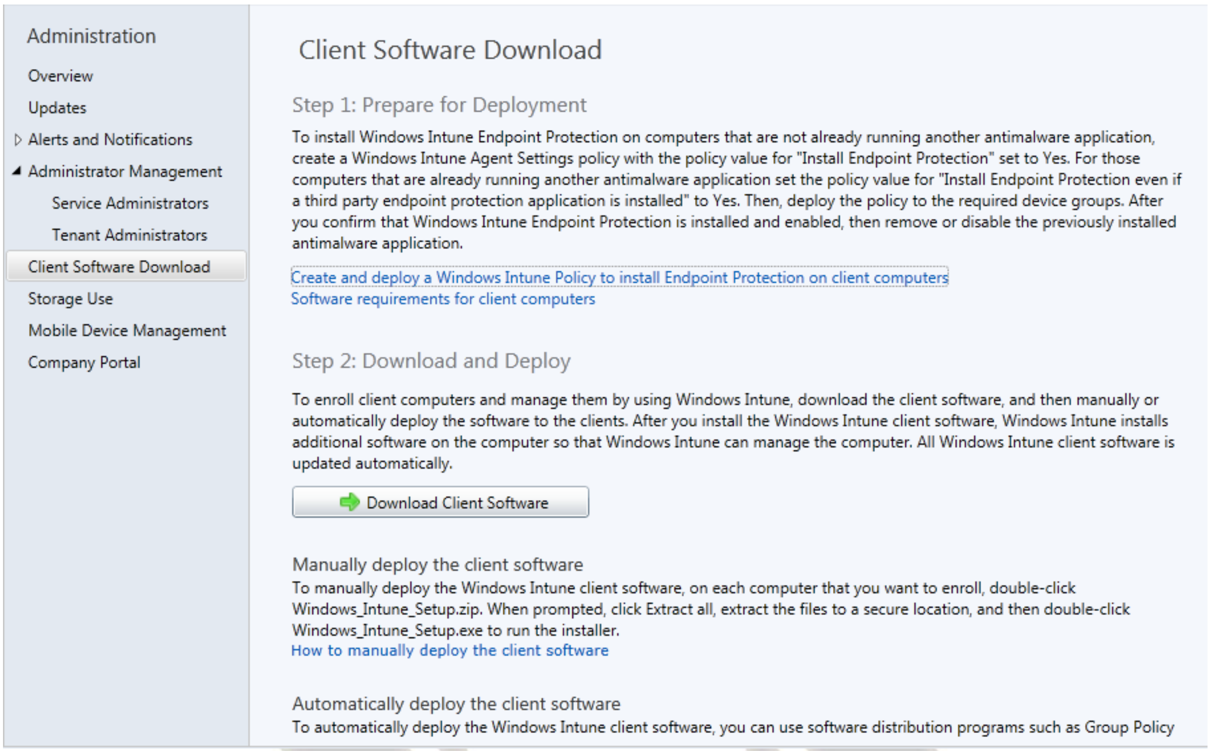
Service Administrators

Service administrators are administrators who are added from within the Windows Intune administrator console. Only users that exist in the Windows Intune administrator console can be service administrators. They can have either of the following levels of access to the console:

- Full access: These service administrators have full administrative rights to the console and can perform all operations in the console, including adding or deleting other service administrators.
- Read-only access: These service administrators have read-only rights and cannot modify data in the console; they can only view data in the console and run reports.

Service administrators cannot manage tenant administrators.

- Client Software Download: Deploy the Windows Intune client software manually or automatically. You can manually install the software on targeted devices that you want to manage with Windows Intune, or you can automate the software deployment to groups of computers by using Group Policy or another automated deployment method. Before you download and deploy the client software, ensure that you have reviewed Planning for Windows Intune Client Deployment and Enrollment.



Client Software Download

Step 1: Prepare for Deployment

To install Windows Intune Endpoint Protection on computers that are not already running another antimalware application, create a Windows Intune Agent Settings policy with the policy value for "Install Endpoint Protection" set to Yes. For those computers that are already running another antimalware application set the policy value for "Install Endpoint Protection even if a third party endpoint protection application is installed" to Yes. Then, deploy the policy to the required device groups. After you confirm that Windows Intune Endpoint Protection is installed and enabled, then remove or disable the previously installed antimalware application.

Create and deploy a Windows Intune Policy to install Endpoint Protection on client computers
Software requirements for client computers

Step 2: Download and Deploy

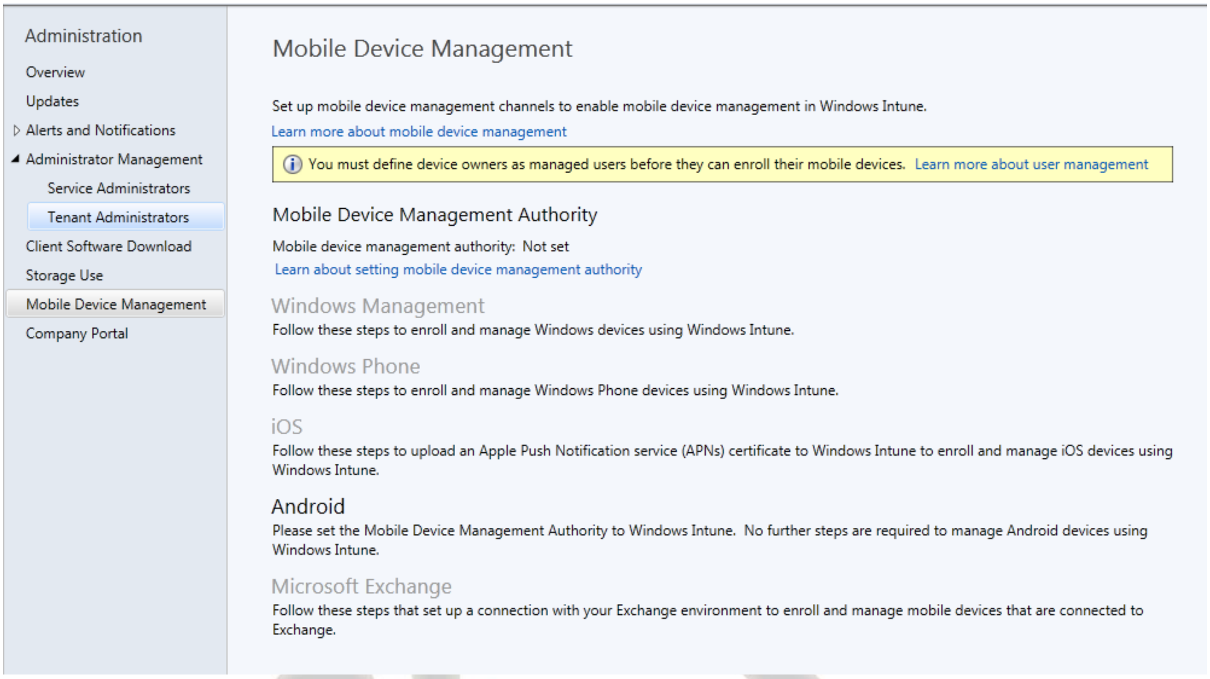
To enroll client computers and manage them by using Windows Intune, download the client software, and then manually or automatically deploy the software to the clients. After you install the Windows Intune client software, Windows Intune installs additional software on the computer so that Windows Intune can manage the computer. All Windows Intune client software is updated automatically.

Manually deploy the client software
To manually deploy the Windows Intune client software, on each computer that you want to enroll, double-click Windows_Intune_Setup.zip. When prompted, click Extract all, extract the files to a secure location, and then double-click Windows_Intune_Setup.exe to run the installer.
How to manually deploy the client software

Automatically deploy the client software
To automatically deploy the Windows Intune client software, you can use software distribution programs such as Group Policy

- Storage Use: View information about or delete managed software applications and updates that have been uploaded to Windows Intune Cloud Storage, and learn how to purchase additional storage. A trial subscription to Windows Intune includes 2 gigabytes (GB) of cloud-based storage that is used to store managed software applications and updates. A paid subscription to Windows Intune includes 20GB of storage per month, with the option to purchase additional storage space at 1GB increments.

- Mobile Device Management: Configure Windows Intune to directly manage mobile devices in your organization, including Windows RT devices, Windows Phone 8 devices, and iOS devices. You can also download the Windows Intune Exchange Connector to set up a connection with your Exchange environment to enroll and manage mobile devices that are connected to Exchange.



Mobile Device Management

Set up mobile device management channels to enable mobile device management in Windows Intune.

Learn more about mobile device management

You must define device owners as managed users before they can enroll their mobile devices. Learn more about user management

Mobile Device Management Authority

Mobile device management authority: Not set

Learn about setting mobile device management authority

Windows Management

Follow these steps to enroll and manage Windows devices using Windows Intune.

Windows Phone

Follow these steps to enroll and manage Windows Phone devices using Windows Intune.

iOS

Follow these steps to upload an Apple Push Notification service (APNs) certificate to Windows Intune to enroll and manage iOS devices using Windows Intune.

Android

Please set the Mobile Device Management Authority to Windows Intune. No further steps are required to manage Android devices using Windows Intune.

Microsoft Exchange

Follow these steps that set up a connection with your Exchange environment to enroll and manage mobile devices that are connected to Exchange.

- Company Portal: Customize the Windows Intune company portal to display your company specific information, such as your company name, contact information for IT support, and URLs for your company privacy statement and internal support website. You can also customize the company portal with your company log, company name, theme colour, and background.

http://technet.microsoft.com/library/jj676683.aspx

Microsoft Desktop Optimization Pack (MDOP)

Microsoft
Desktop Optimization Pack
for Software Assurance
Asset Inventory Service
Advanced Group Policy Management
Application Virtualization
System Center Desktop Error Monitoring
Diagnostics and Recovery Toolset
Enterprise Desktop Virtualization

The Microsoft Desktop Optimization Pack (MDOP) is a suite of technologies available as a subscription for Software Assurance customers. MDOP virtualization technologies help personalize the user experience, simplify application deployment, and improve application compatibility with the Windows operating system **(UE-V/App-V/MED-V).** Additionally, MDOP helps you manage and secure your device, enabling monitoring, and deployment of key Windows features **(MBAM/AGPM)**. Using MDOP shifts desktop repair from reactive to proactive, saving time and removing challenges associated with troubleshooting and repairing system failures **(DaRT).**

Application Virtualization (APP-V)

Microsoft Application Virtualization (App-V) can make applications available to end user computers without having to install the applications directly on those computers. This is made possible through a process known as *sequencing the application*, which enables each application to run in its own self-contained virtual environment on the client computer. The sequenced applications are isolated from each other. This eliminates application conflicts, but the applications can still interact with the client computer.

The App-V client is the feature that lets the end user interact with the applications after they have been published to the computer. The client manages the virtual environment in which the virtualized applications run on each computer. After the client has been installed on a computer, the applications must be made available to the computer through a process known as *publishing*, which enables the end user to run the virtual applications. The publishing process copies the virtual application icons and shortcuts to the computer—typically on the Windows desktop or on the **Start** menu—and also copies the package definition and file type association information to the computer. Publishing also makes the application package content available to the end user's computer.

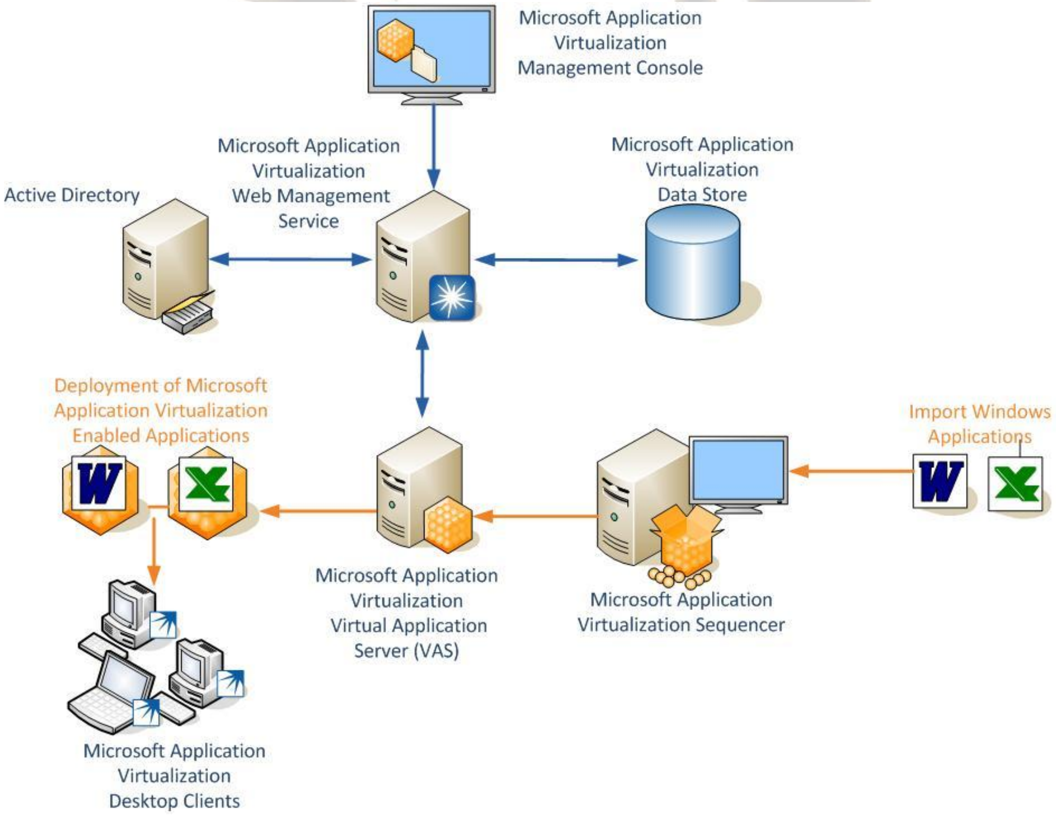
The virtual application package content can be copied onto one or more Application Virtualization servers so that it can be streamed down to the clients on demand and cached locally. File servers and Web servers can also be used as streaming servers, or the content can be copied directly to the end user's computer—for example, if you are using an electronic software distribution system, such as Microsoft System Center Configuration Manager. In a multi-server implementation, maintaining the package content and keeping it up to date on all the streaming servers requires a comprehensive package management solution. Depending on the size of your organization, you might need to have many virtual applications available to end users located all over the world. Managing the packages to ensure that the appropriate applications are available to all users where and when they need access to them is therefore an important requirement.

The Microsoft Application Virtualization (App-V) infrastructure includes:

•App-V Sequencer—The App-V Sequencer converts application data into a format that is compatible with the App-V server and client, producing an App-V application.

•App-V Server—An App-V application can be placed on one or more App-V servers so that it can be streamed down to the clients on demand and cached locally.

•App-V Client—The App-V Client is the system component that enables the end user to interact with the App-V applications that are available on the App-V server.


Microsoft Application Virtualization Management Console
Microsoft Application Virtualization Web Management Service
Active Directory
Microsoft Application Virtualization Data Store
Deployment of Microsoft Application Virtualization Enabled Applications
Import Windows Applications
Microsoft Application Virtualization Virtual Application Server (VAS)
Microsoft Application Virtualization Sequencer
Microsoft Application Virtualization Desktop Clients

Microsoft Enterprise Desktop Virtualization (MED-V)

Windows 7 Support Only

When upgrading to a new version of Windows, enterprises must first inventory and test line of business applications on the new operating system and your organization may have some applications that are not yet officially supported by your vendor, or might not work at all despite all efforts.

This whole process of testing, fixing the application, upgrading to a new version that supports Windows 7 or finding an alternative application can be time-consuming. Meanwhile, users are unable to take advantage of the operating system's new capabilities and enhancements, and IT departments have to delay upgrade plans. Microsoft Enterprise Desktop Virtualization (MED-V) can help ease these challenges. Some of the key benefits of MED-V are:

- Maintaining business continuity:

MED-V removes the barriers to Windows upgrades by resolving application incompatibility with Windows 7 and delivering applications in a Windows XP-based application compatibility workspace. Upgrades can proceed on schedule, and users can take advantage of the power of Windows 7 right away without losing access to applications they need while IT departments can remediate incompatible applications.

- Easy to use:

MED-V enables users to seamlessly start the legacy applications right from the Windows Start. Applications appear and operate as if they were installed on the desktop or pinned to the task bar. In MED-V 2.0 legacy applications share seamless access to user documents and network-available printers, and even USB devices such as flash storage or Smartcard readers.

- Simplified IT management:

MED-V is easy to deploy and manage. MED-V 2.0 integrates with existing management and deployment systems, such as System Center Configuration Manager, for easy, scalable, enterprise deployment.

The MED-V solution comprises the following elements:

• Administrator-defined virtual machine—Encapsulates a full desktop environment, including an operating system, applications, and optional management and security tools.

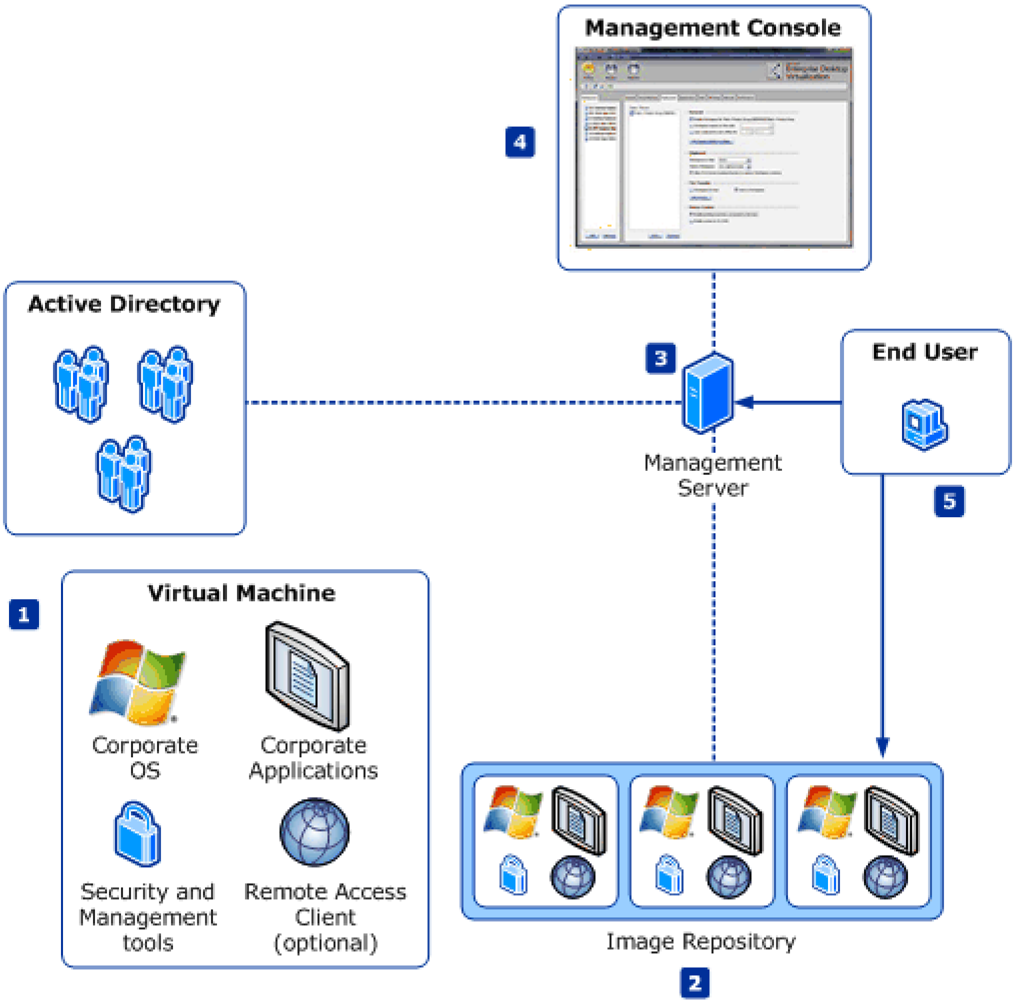
• Image repository—Stores all virtual images on a standard IIS server and enables virtual images version management, client-authenticated image retrieval, and efficient download (of a new image or updates) via Trim Transfer technology.

• Management server—Associates virtual images from the image repository along with administrator usage policies to Active Directory® users or groups. The management server also aggregates clients' events and stores them in an external database (Microsoft SQL Server®) for monitoring and reporting purposes.

• Management console—Enables administrators to control the management server and the image repository.

• End-user client

- Virtual image life-cycle—Authentication, image retrieval, enforcement of usage policies.
- Virtual machine session management—Start, stop, lock the virtual machine.
- Single desktop experience—Applications installed in the virtual machine seamlessly available through the standard desktop Start menu and integrated with other applications on the user desktop.



Microsoft Bitlocker Administration and Monitoring (MBAM)

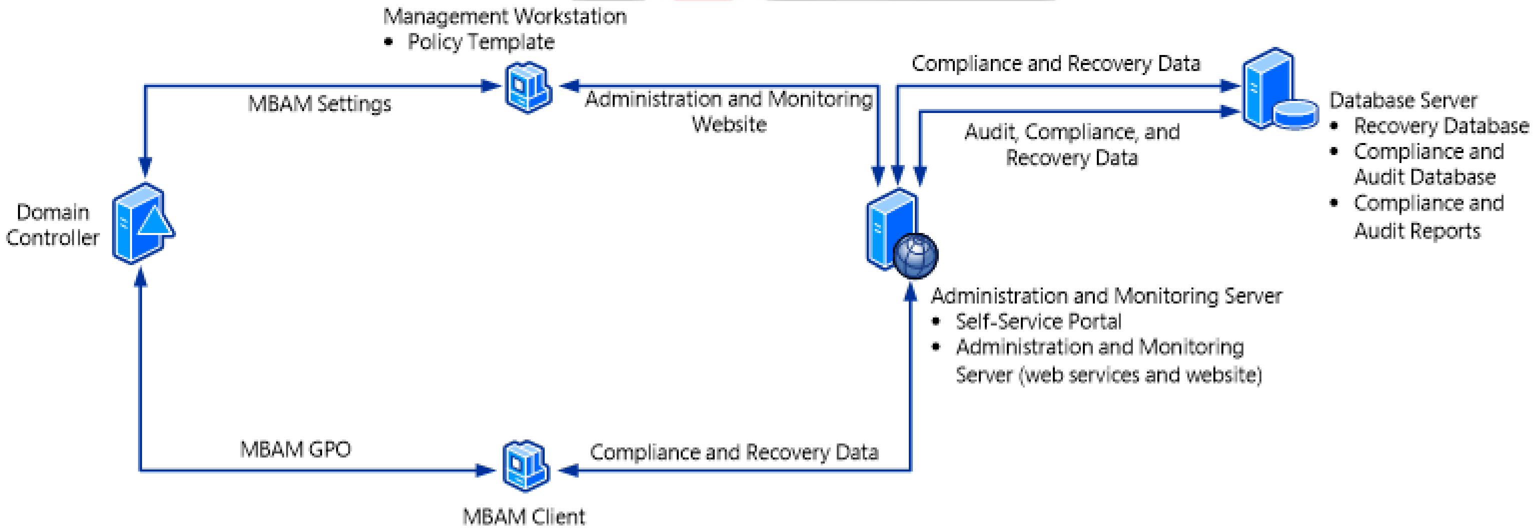
Microsoft BitLocker Administration and Monitoring (MBAM) provides enterprise management capabilities for BitLocker and BitLocker to Go. MBAM simplifies deployment and key recovery, provides centralized compliance monitoring and reporting, and minimizes the costs associated with provisioning and supporting encrypted drives within your organization.

Microsoft BitLocker Administration and Monitoring (MBAM) is a client/server solution that can help you simplify BitLocker provisioning and deployment, improve compliance and reporting on BitLocker, and reduce support costs.

Microsoft BitLocker Administration and Monitoring can be deployed in the Stand-alone topology, or in a topology that is integrated with Microsoft System Center Configuration Manager 2007 or Microsoft System Center 2012 Configuration Manager.

The following diagram shows the MBAM recommended architecture for a production environment, which consists of two servers and a management workstation. This architecture supports up to 200,000 MBAM clients. The server features and databases in the architecture image are described in the following section.

Note



Management Workstation
• Policy Template
MBAM Settings
Administration and Monitoring Website
Compliance and Recovery Data
Audit, Compliance, and Recovery Data
Database Server
• Recovery Database
• Compliance and Audit Database
• Compliance and Audit Reports
Domain Controller
Administration and Monitoring Server
• Self-Service Portal
• Administration and Monitoring Server (web services and website)
MBAM GPO
Compliance and Recovery Data
MBAM Client

A single-server architecture should be used only in test environments.

Administration and Monitoring Server

The following features are installed on this server:

- **Administration and Monitoring Server**. The Administration and Monitoring Server feature is installed on a Windows server and consists of the Administration and Monitoring website, which includes the reports and the Help Desk Portal, and the monitoring web services.
- **Self-Service Portal**. The Self-Service Portal is installed on a Windows server. The Self-Service Portal enables end users on client computers to independently log on to a website, where they can obtain a recovery key to recover a locked BitLocker volume.

Database Server

The following features are installed on this server:

- **Recovery Database**. The Recovery Database is installed on a Windows server and a supported instance of Microsoft SQL Server. This database stores recovery data that is collected from MBAM client computers.
- **Compliance and Audit Database**. The Compliance and Audit Database is installed on a Windows server and a supported instance of SQL Server. This database stores compliance data for MBAM client computers. This data is used primarily for reports that SQL Server Reporting Services (SSRS) hosts.
- **Compliance and Audit Reports**. The Compliance and Audit Reports are installed on a Windows server and a supported instance of SQL Server that has the SQL Server Reporting Services (SSRS) feature installed. These reports provide MBAM reports that you can access from the Administration and Monitoring website or directly from the SSRS server.

Management Workstation

The following feature is installed on the Management workstation, which can be a Windows server or a client computer.

- **Policy Template**. The Policy Template consists of Group Policy settings that define MBAM implementation settings for BitLocker drive encryption. You can install the Policy template on any server or workstation, but it is commonly installed on a management workstation, which is a supported Windows server or client computer. The workstation does not have to be a dedicated computer.

MBAM Client

The MBAM Client is installed on a Windows computer and has the following characteristics:

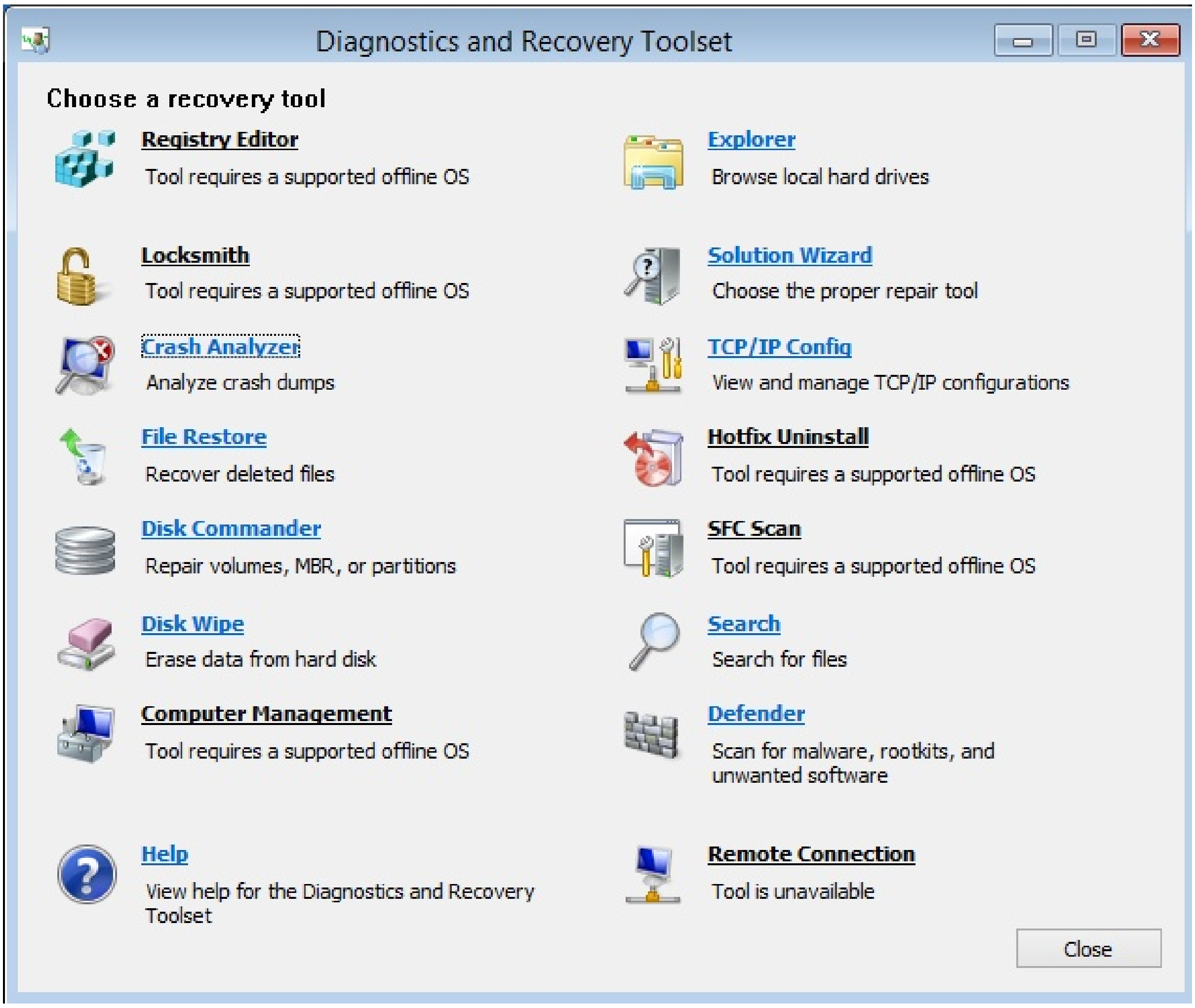
- Uses Group Policy to enforce the BitLocker drive encryption of client computers in the enterprise.
- Collects the recovery key for the three BitLocker data drive types: operating system drives, fixed data drives, and removable data (USB) drives.
- Collects compliance data for the computer and passes the data to the reporting system.

Windows Diagnostic and Recovery Toolset (DaRT)

Microsoft Diagnostics and Recovery Toolset (DaRT) allows you diagnose and repair a computer that cannot be started or that has problems starting as expected. By using DaRT, you can recover end-user computers that have become unusable, diagnose probable causes of issues, and quickly repair unbootable or locked-out computers. When it is necessary, you can also quickly restore important lost files and detect and remove malware, even when the computer is not online.

DaRT lets you create a DaRT recovery image in International Organization for Standardization (ISO) and Windows Imaging (WIM) file formats and burn the image to a CD, DVD, or USB. You can then use the recovery image files and deploy them locally or to a remote partition or a recovery partition.

DaRT tools



Choose a recovery tool

Registry Editor
Tool requires a supported offline OS

Explorer
Browse local hard drives

Locksmith
Tool requires a supported offline OS

Solution Wizard
Choose the proper repair tool

Crash Analyzer
Analyze crash dumps

TCP/IP Config
View and manage TCP/IP configurations

File Restore
Recover deleted files

Hotfix Uninstall
Tool requires a supported offline OS

Disk Commander
Repair volumes, MBR, or partitions

SFC Scan
Tool requires a supported offline OS

Disk Wipe
Erase data from hard disk

Search
Search for files

Computer Management
Tool requires a supported offline OS

Defender
Scan for malware, rootkits, and unwanted software

Help
View help for the Diagnostics and Recovery Toolset

Remote Connection
Tool is unavailable

- Computer Management

Computer Management is a collection of Windows administrative tools that help you troubleshoot a problem computer. You can use the Computer Management tools in DaRT to view system information and event logs, manage disks, list autoruns, and manage services and drivers. The Computer Management console is customized to help you diagnose and repair problems that might be preventing the Windows operating system from starting.

The recovery of dynamic disks with DaRT is not supported.

- Crash Analyzer

Use the Crash Analyzer Wizard to quickly determine the cause of a computer failure by analyzing the memory dump file on the Windows operating system that you are repairing. Crash Analyzer examines the memory dump file for the driver that caused a computer to fail. You can then disable the problem device driver by using the Services and Drivers node in the Computer Management tool.

The Crash Analyzer Wizard requires the Debugging Tools for Windows and symbol files for the operating system that you are repairing. You can include both requirements when you create the DaRT recovery image. If they are not included on the recovery image and you do not have access to them on the computer that you are repairing, you can copy the memory dump file to another computer and use the stand-alone version of Crash Analyzer to diagnose the problem.

Running Crash Analyzer is a good idea even if you plan to reimage the computer. The image could have a defective driver that is causing problems in your environment. By running Crash Analyzer, you can identify problem drivers and improve the image stability.

- Defender

Defender can help detect malware and unwanted software and warn you of security risks. You can use this tool to scan a computer for and remove malware even when the installed Windows operating system is not running. When Defender detects malicious or unwanted software, it prompts you to remove, quarantine, or allow for each item.

Malware that uses rootkits can mask itself from the running operating system. If a rootkit-enabled virus or spyware is in a computer, most real-time scanning and removal tools can no longer see it or remove it. Because you boot the problem computer into DaRT and the installed operating system is offline, you can detect the rootkit without it being able to mask itself.

- Disk Commander

Disk Commander lets you recover and repair disk partitions or volumes by using one of the following recovery processes:

- Restore the master boot record (MBR)
- Recover one or more lost volumes
- Restore partition tables from Disk Commander backup
- Save partition tables to Disk Commander backup

The recovery of dynamic disks with DaRT is not supported

- Disk Wipe

You can use Disk Wipe to delete all data from a disk or volume, even the data that is left behind after you reformat a hard disk drive. Disk Wipe lets you select from either a singlepass overwrite or a four-pass overwrite, which meets current U.S. Department of Defense standards.

After wiping a disk or volume, you cannot recover the data. Verify the size and label of a volume before erasing it.

- Explorer

The Explorer tool lets you browse the computer's file system and network shares so that you can remove important data that the user stored on the local drive before you try to repair or reimage the computer. And because you can map drive letters to network shares, you can easily copy and move files from the computer to the network for safekeeping or from the network to the computer to restore them.

- File Restore

File Restore lets you try to restore files that were accidentally deleted or that were too big to fit in the Recycle Bin. File Restore is not limited to regular disk volumes, but can find and restore files on lost volumes or on volumes that are encrypted by BitLocker.

- File Search

Before reimaging a computer, recovering files from the local hard disk is important, especially when the user might not have backed up or stored the files elsewhere.

The Search tool opens a File Search window that you can use to find documents when you do not know the file path or to search for general kinds of files across all local hard disks. You can search for specific file-name patterns in specific paths. You can also limit results to a date range or size range.

- Hotfix Uninstall

The Hotfix Uninstall Wizard lets you remove hotfixes or service packs from the Windows operating system on the computer that you are repairing. Use this tool when a hotfix or service pack is suspected in preventing the operating system from starting.

It is recommended that you uninstall only one hotfix at a time, even though the tool lets you uninstall more than one.

- Locksmith

The Locksmith Wizard lets you set or change the password for any local account on the Windows operating system that you are analysing or repairing. You do not have to know the current password. However, the password that you set must comply with any requirements that are defined by a local Group Policy Object. This includes password length and complexity.

You can use Locksmith when the password for a local account, such as the local Administrator account, is unknown. *You cannot use Locksmith to set passwords for domain accounts.*

- Registry Editor

You can use Registry Editor to access and change the registry of the Windows operating system that you are analysing or repairing. This includes adding, removing, and editing keys and values, and importing registry (.reg) files.

Serious problems can occur if you change the registry incorrectly by using Registry Editor. These problems might require you to reinstall the operating system. Before you make changes to the registry, you should back up any valued data on the computer. Change the registry at your own risk.

- SFC Scan

The SFC Scan tool starts the System File Repair Wizard and lets you repair system files that are preventing the installed Windows operating system from starting. The System File Repair Wizard can automatically repair system files that are corrupted or missing, or it can prompt you before it performs any repairs.

- Solution Wizard

The Solution Wizard presents a series of questions and then recommends the best tool for the situation, based on your answers. This wizard helps you determine which tool to use when you are not familiar with the tools in DaRT.

- TCP/IP Config

When you boot a problem computer into DaRT, it is set to automatically obtain its TCP/IP configuration (IP address and DNS server) from Dynamic Host Configuration Protocol (DHCP). If DHCP is unavailable, you can manually configure TCP/IP by using the TCP/IP Config tool. You first select a network adapter, and then configure the IP address and DNS server for that adapter.