

TechNet TV

Windows 8.1

BYODiin liittyvät ominaisuudet

Petri Paavola
Windows Client MVP
Names.fi
22.10.2013



Petri Paavola
Windows Client MVP



Petri.Paavola@names.fi

Names
BY ENTER

Windows 8.1 BYOD-käytössä



Web Application Proxy
Workplace Join
Multi-factor Authentication
Work Folders
Mobile Device Management
Open MDM
RDS- & VDI-parannukset
Windows To Go

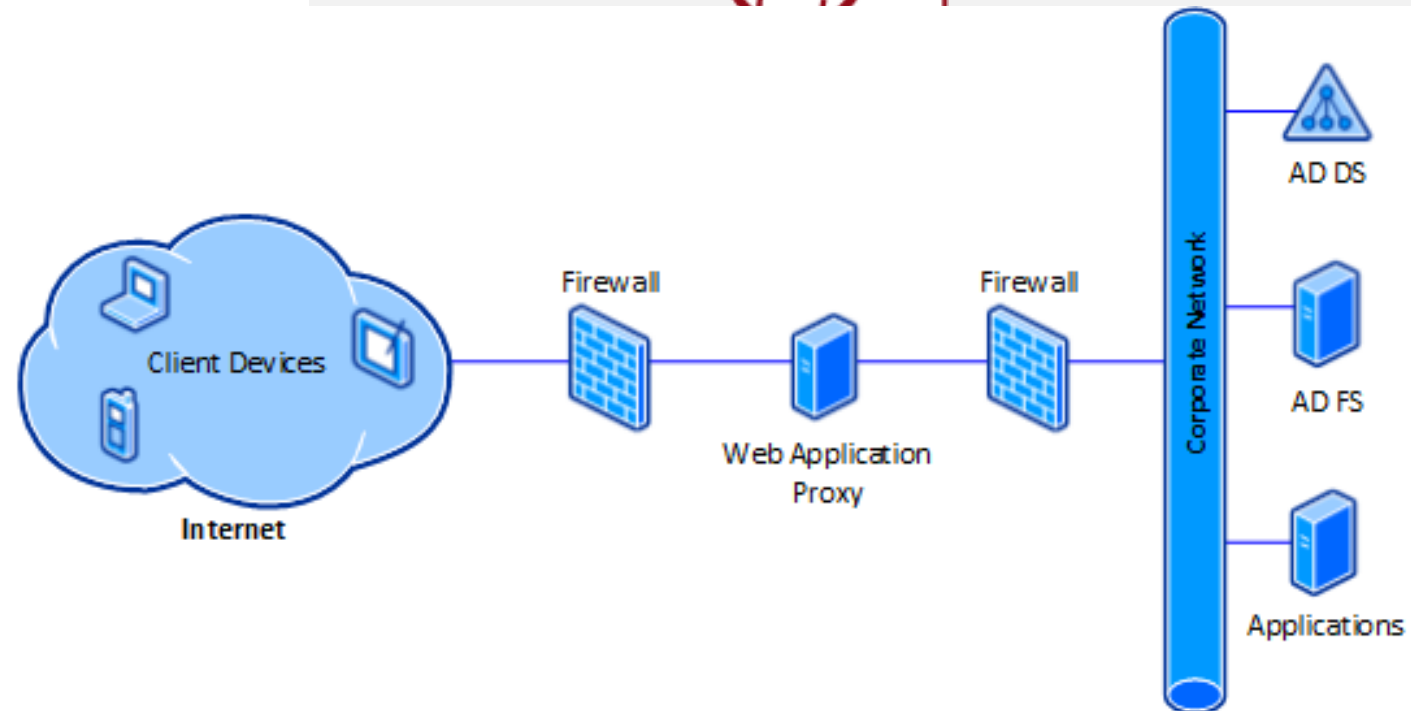
Web Application Proxy

Publish web-based applications through reverse proxy

AD FS based Single Sign-On (SSO)

Multifactor authentication

Multifactor access control



Windows 8.1: Workplace Join



Manage access to company data

Register personal devices

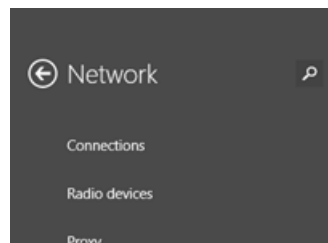
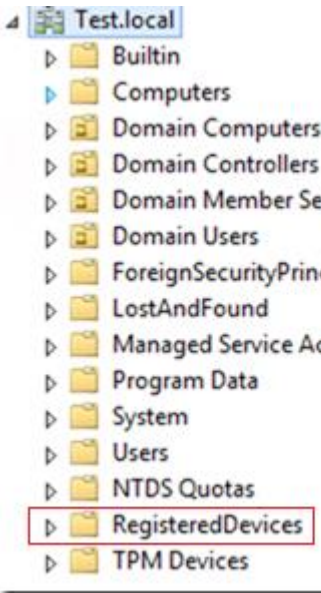
Simple for the employee

Device enrollment with ADFS

Workplace join



- Käyttäjän oman laitteen "kytkentä" toimialueeseen ilman että laite tulee toimialueen hallintaan
- Standalone ja Domain Joined välimaastossa
- Tarjoaa tietoturvaa ja helpon pääsyn valittuihin toimialueen www-pohjaisiin palveluihin SingleSignOnin kautta
- Käyttää ADFS:ää
- Clientit: Windows 8.1 ja iOS tällä hetkellä
- AD:hen luodaan koneelle oma koneobjekti (RegisteredDevices)
- Samassa yhteydessä luodaan laitekohtainen varmenne, minkä avulla käyttäjä/laite tunnistetaan myöhemmin



Workplace

Join your workplace network so that you can use network resources like internal websites and business apps

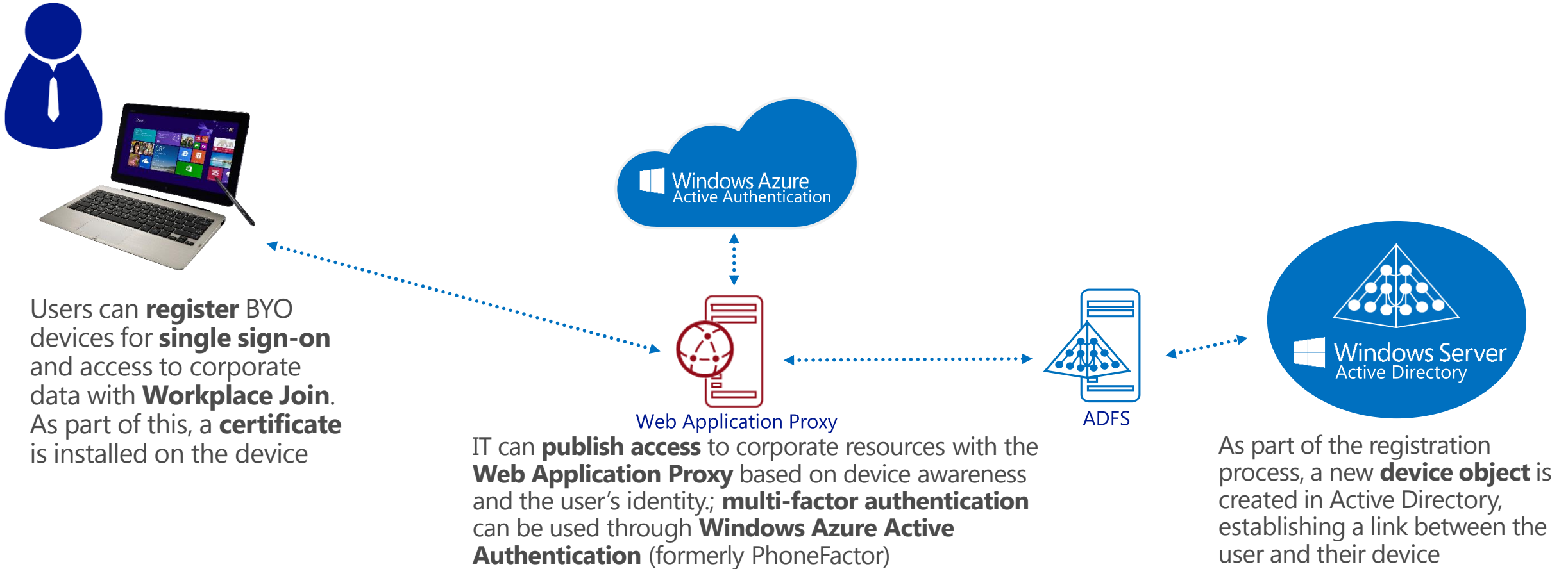
Join

Workplace join



- Laitteelle voidaan antaa pääsyjä organisaation sisäisiin resursseihin
- Koska laite tunnistetaan, voidaan luoda second factor authentication (lisää tästä myöhemmin) ja myös Single-Sign-On saadaan käyttöön
- esim. vaaditaan, että external-yhteydenotot täytyy tehdä varmenteilla (tunnettu kone Workplace Joinattu) sekä lisäksi vielä tietty AD-ryhmä (Multifactor Access Control certification+AD-group)
- Käyttäjällä täysi hallinta, voi itse poistaa laitteen kytkennän milloin vain.

Workplace Join



Multi-Factor Authentication (MFA)

- Käyttäjän vahvennettu autentikointi julkaistuuun resurssiin
- Pääsynhallinnassa vaaditaan käyttäjän tunnistuksen lisäksi myös jokin toinen autentikointimuoto
- Toinen autentikointi voi olla esim. kertakäyttösalasana, älykortti, varmenne.
- Web Application Proxy ja AD FS voidaan konfiguroida vaatimaan MFA aina tai se voidaan kohdistaa tiettyihin resursseihin.
- Esim. voidaan vaatia sekä käyttäjän että laitteen tunnistus. Näin voidaan konfiguroida vaatimukseksi external verkon pääsulle käyttäjän tunnus/salasana sekä Workplace Joined laite, joka tunnistetaan varmenteen perusteella.
- Edelliseen voidaan vielä lisätä, että käyttäjä pitää olla rekisteröity juurikin ko. laitteen käyttäjäksi (Admin voi rekisteröidä, jolloin hallinta IT:llä)

Multi-Factor Access Control

- ADFS taustalla
- ADFS luo Tokeneita, jotka sisältävät Claimeja (claims).
- Claimeja voidaan yhdistää säännöillä
- ADFS-turvattu (www-)applikaation pääsynhallintaa voidaan määritellä joustavasti säännöillä (useampi sääntö, joiden pitää toteutua)

Esimerkiksi:

Yksinkertainen malli: Käyttäjä pääsee resurssiin käsiksi, jos hän kuuluu tiettyyn AD-ryhmään

Advanced:

Permit access to an application secured by AD FS only if the access request is coming from a workplace joined device that is registered to the user

Permit access to an application secured by AD FS only if the access request is coming from a workplace joined device that is registered to a user whose identity has been validated with MFA

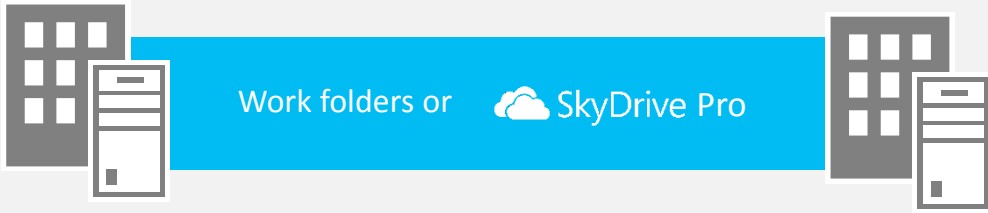
Manage Risk with Multi-Factor Access Control

<http://technet.microsoft.com/en-us/library/dn280937.aspx>

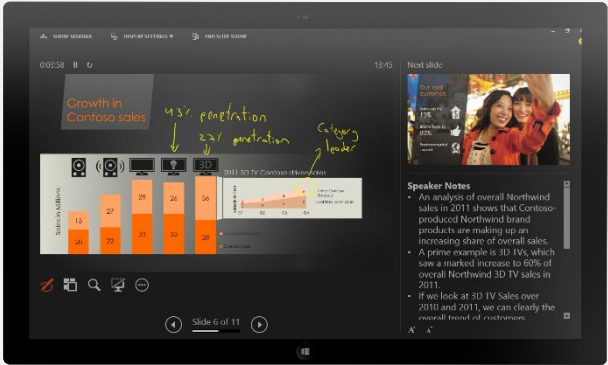
Windows Azure Multi-Factor Authentication

- Ja vielä yksi erilainen Multi-Factor Authentication.
- Sama ajatus, halutaan tunnistaa käyttäjä useammalla kuin yhdellä tavalla ennen kuin annetaan pääsy resursseihin
- 3 eri tapaa tehdä: Applikaatio, tekstiviesti (jossa salasana), automaattinen puhelu
- Voidaan käyttää On-premise –palveluissa, pilvipalveluissa kuten Windows Azure, Office 365 ja Dynamics CRM sekä omat itse tehdyt sovellukset
- DEMO

Work Folders with you



Lost or Damaged Device



Used on Old Device
Replacement Device

Work Folders



Work Folders provides a single point of access to work files on a user's work and personal devices



Control Panel->System and Security->Work Folders

Work Folders tukee alkuvaiheessa Win 8.1 ja RT laitteita, myöhemmin tuettuja alustoja lisätään

The biggest difference from SkyDrive or SkyDrive Pro is that the centralized storage for Work Folders is an on-premise file server running Windows Server 2012 R2. Work Folder use HTTPS protocol and designed for the individual work data (no sharing sync files with other users)

• Work Folders



Work Folders

	Consumer / personal data	Individual work data	Team / group work data	Personal devices	Access Protocol	Data location
SkyDrive	x			x	HTTPS	Public cloud
SkyDrive Pro		x	x	x	HTTPS	SharePoint / Office 365
Work Folders		x		x	HTTPS	File server
Folder Redirection / Client-Side Caching		x			SMB (only form on-prem or using VPN)	File server

- Administrators can use Work Folders to provide users with access to their work files while **keeping centralized storage and control over the organization's data**. Provide access work files while offline and sync with the central file server when the PC or device next has Internet or network connectivity. Use existing file server management technologies such as **file classification and folder quotas** to manage user data. Use **Failover Clustering** with Work Folders to provide high-availability solution

Remote Business Data Removal

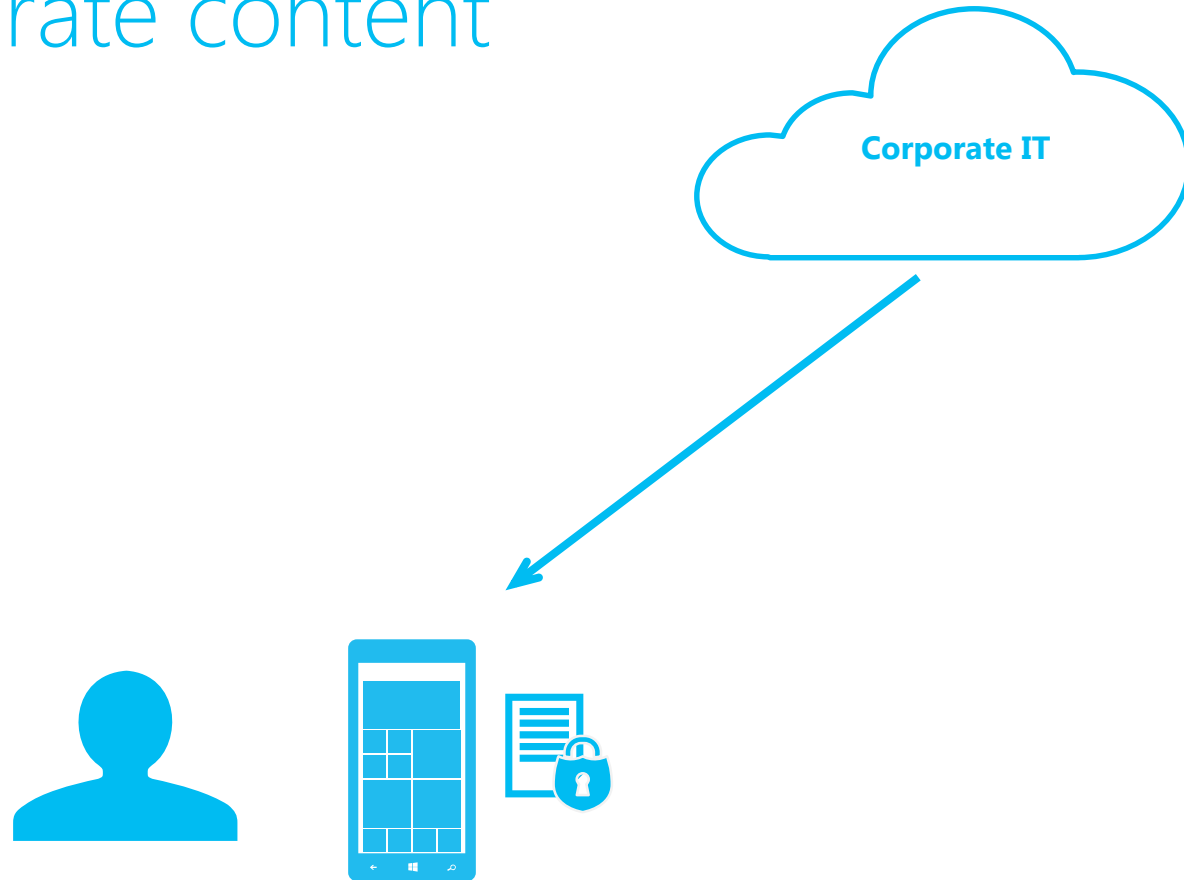
More control of corporate content

Device can be wiped

Encrypted

EAS

EAS+ OMA-DM



Mobile Device Management



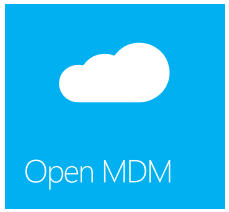
Kone Intunen hallintaan ilman konekohtaisen clientin asennusta

Käyttäjän omistamaan Windows 8.1 -laitteeseen voidaan laittaa tarjolle organisaation sovelluksia (Company Portal)

Käyttäjän "enrollaamaa" laitetta hallitaan kuin mobiililaitetta (vs. täysin hallittu ConfigMgr, joka tarvitsee hallinta-agentin)

Laajempi Windows RT:n hallinta

Open Mobile Device Management (MDM)



Windows 8.1 –laitteita voidaan hallita kuin ne olisivat mobiililaitteita

Based on open standards (OMA-DM)

Uses Open Mobile Alliance Device Management protocols

Secure communication with cloud-based management

No additional agent required in Windows 8.1 and Windows RT 8.1

Implemented by multiple ISVs

Microsoft (Windows Intune)

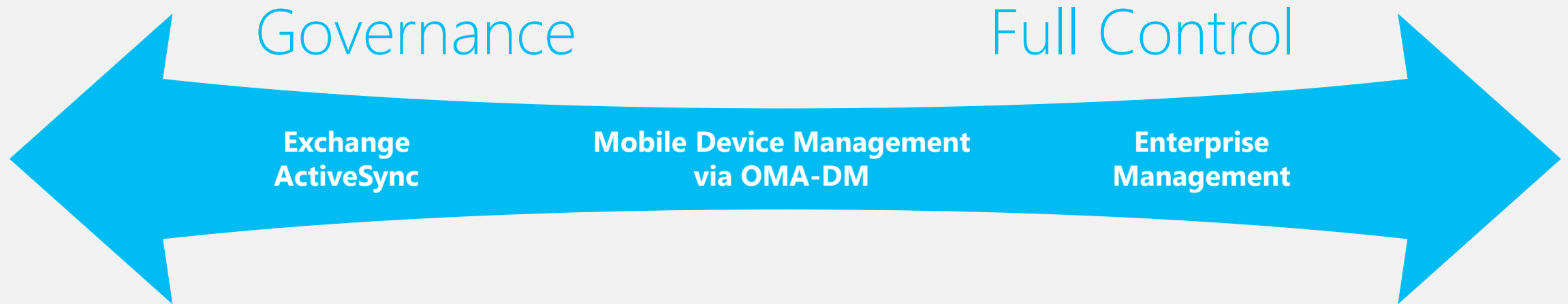
Airwatch

Mobile Iron

Open protocol enables implementation by additional vendors



Managing Windows Devices



Windows 8.1 provides choices

Choose by device based on scenario or capabilities needed
Consider employee versus organization-owned, BYOD, connectivity
Organizations may choose all three

Remote Desktop Services

- RDS-rooli sisältää sekä vanhan terminaalipöydän (Remote Desktop), että VDI-virtuaalikoneet (dedikoidut ja pooled).
- RemoteApp –sovellukset käyttäytyvät entistä enemmän kuin olisivat paikallisesti asennettuja.
- RDS palveluiden käyttö hitaiden verkkoyhteyksien yli on parantunut (faster reconnects and improved compression)
- Kosketusnäyttötuki, multimedia, grafiikka, USB-tuki
- Multi-monitor tuki on parantunut.
- Palvelinpuolella merkittäviä parannuksia, mm. levyn deduppaus

Remote Desktop –clientit Android, iOS ja OSX

Microsoft Remote Desktop –appsit Androidille, iOS:lle sekä Mac OS X:lle

Android: <https://play.google.com/store/apps/details?id=com.microsoft.rdc.android&hl=fi>

iOS: <https://itunes.apple.com/fi/app/id714464092?mt=8&affId=2064962>

Mac OS X: <https://itunes.apple.com/us/app/microsoft-remote-desktop/id715768417?mt=12>

Sekä etätyöpöytä, että julkaistut sovellukset

RemoteFX

Haluat oikeasti käyttää Windows Server 2012R2 RDS –palvelinta.

Kokeillaanpas 😊

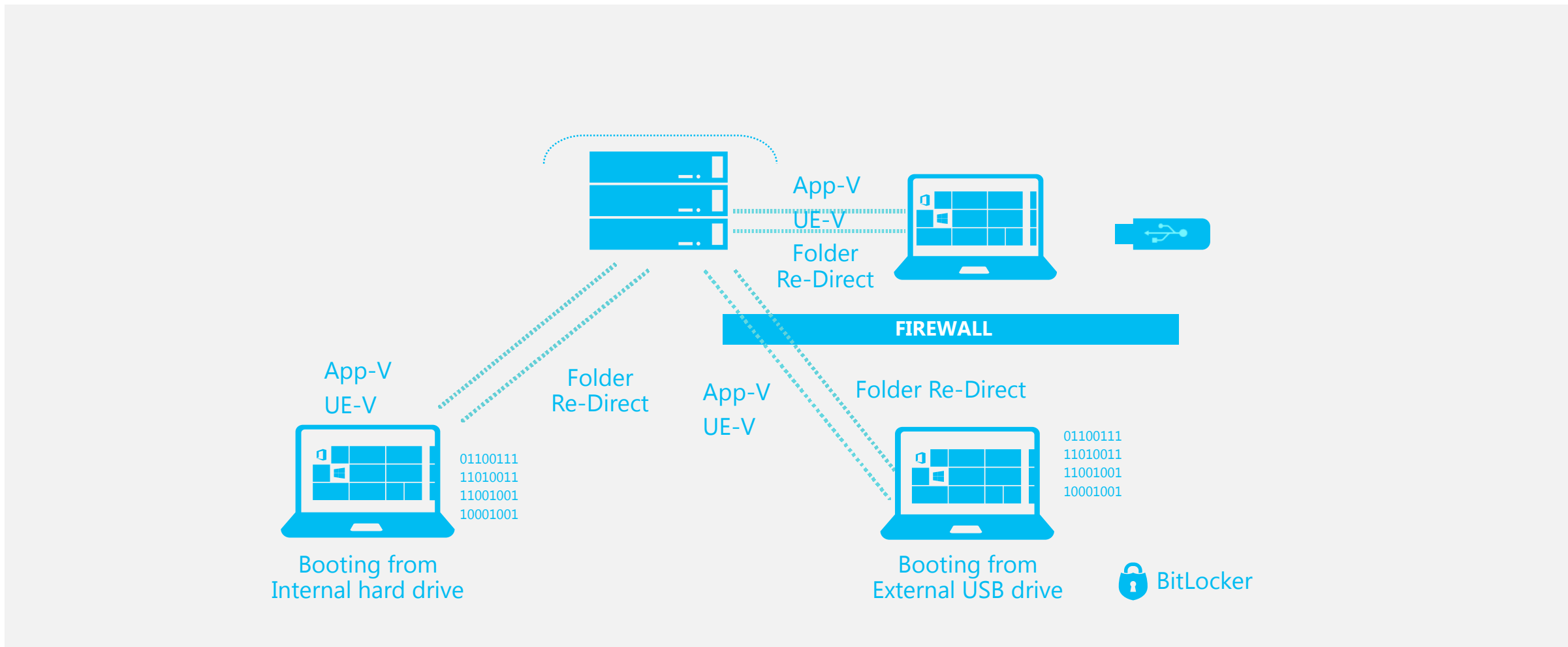
Windows To Go

BYODia kauneimmillaan



Windows To Go, Your Portable Workspace

A consistent Windows 8.1 experience on any device with Windows To Go



* Any device certified for use with Windows 7, Windows 8, or Windows 8.1, regardless of the OS running on the host machine. Software Assurance (SA) for Windows required .

Mobility for the Enterprise

Windows To Go: Windows in your back pocket

**Kuudes skenaario:
Windows 8.1:n
testaus/käyttöönotto
jyräämättä koneita**



Contractors



Bring Your Own
Device (at work)



Travel Light /
Work from Home

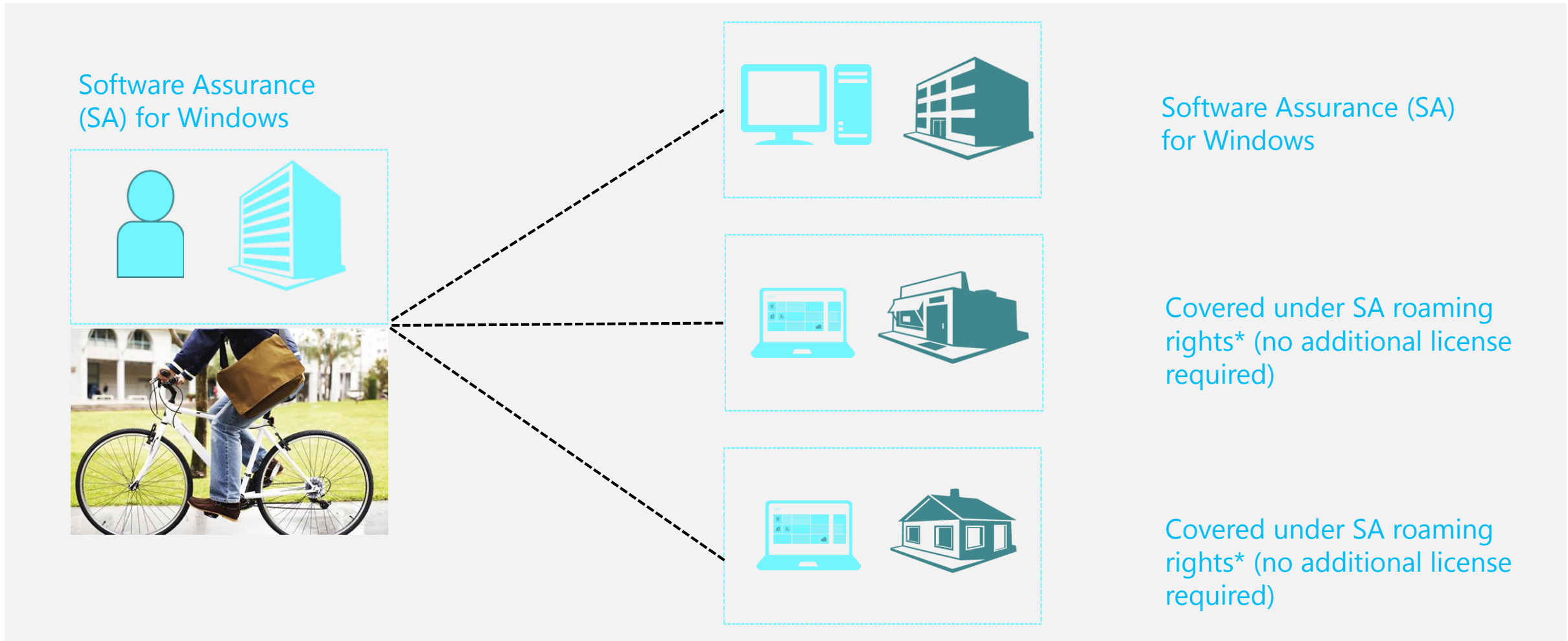


Shared PCs



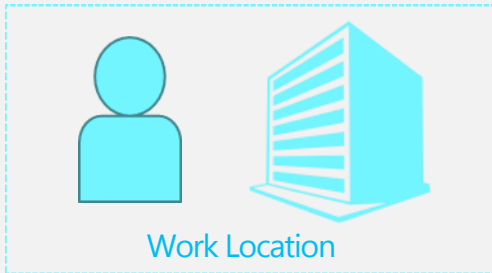
Up and Running
on Windows 8

Travel Light: At work, at home, on the road



*Roaming rights provide the primary user of an SA covered device rights to run Windows To Go or VDI from non-corp devices while off premise.

Bring Your Own Device; Employees and Contingent Staff



Primary Device



Windows VDA or Software Assurance (SA) for Windows

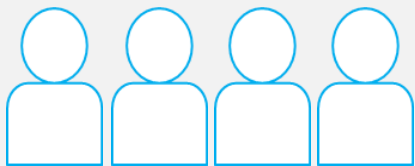
Secondary Device



Companion Subscription License (CSL)*

*Windows CSL provides the primary user of an SA or VDA covered device rights to run Windows To Go or VDI from secondary non-corp owned devices.

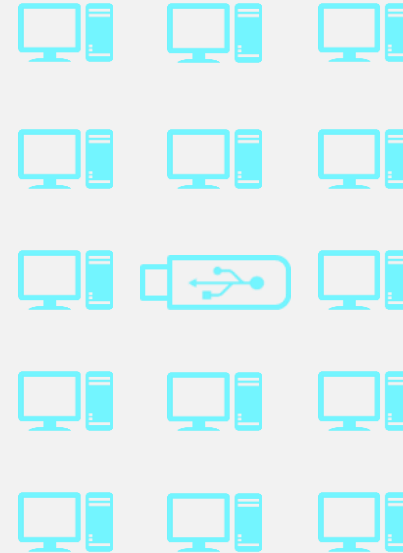
Shared PCs



Multiple Users



Single or Multiple Locations



Shared PCs

Software Assurance (SA) for Windows

Windows in your back pocket

Secure

Easy To Use

Manageable

Protecting corporate data

Supports BitLocker drive encryption

New Password Key Protector

Pre-OS password to unlock Windows To Go

Trusted Platform Module (TPM) is not used

MDOP 2013 and MBAM

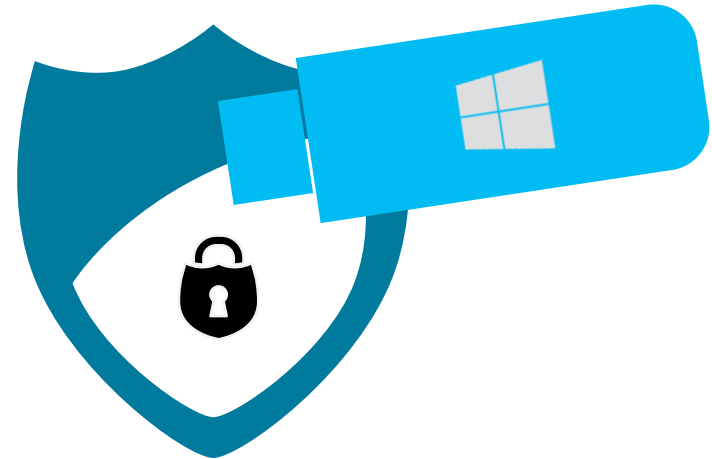
Protection with Trusted Boot

Protects Windows boot process and anti-malware software

Protection with Windows

Can take advantage of all Windows security offerings, just like a laptop

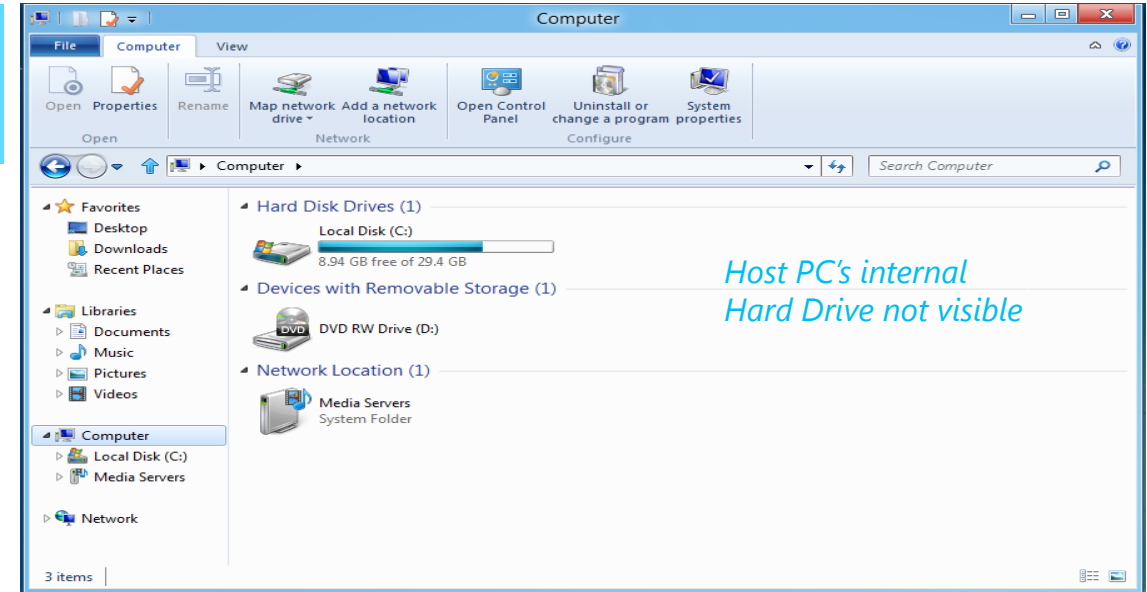
For example, remote connectivity solutions still enforce the same security requirements



Secure: Prevents data leakage

Separation from host PC's internal hard drive

- Makes the host's internal hard drive offline
- External Storage Devices are still accessible
- Utilizes SAN policy
- Can be controlled by Group Policy



Booting from USB

Windows To Go Startup Options

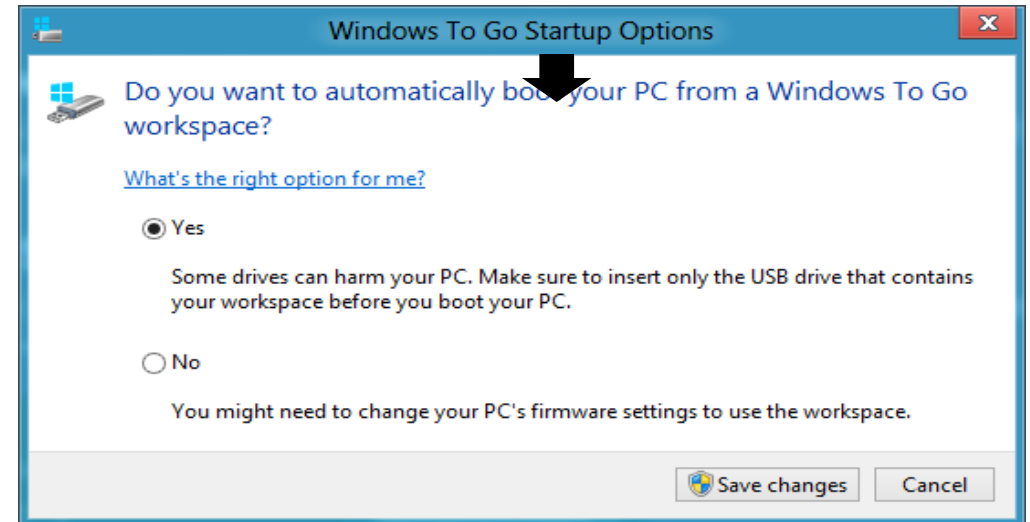
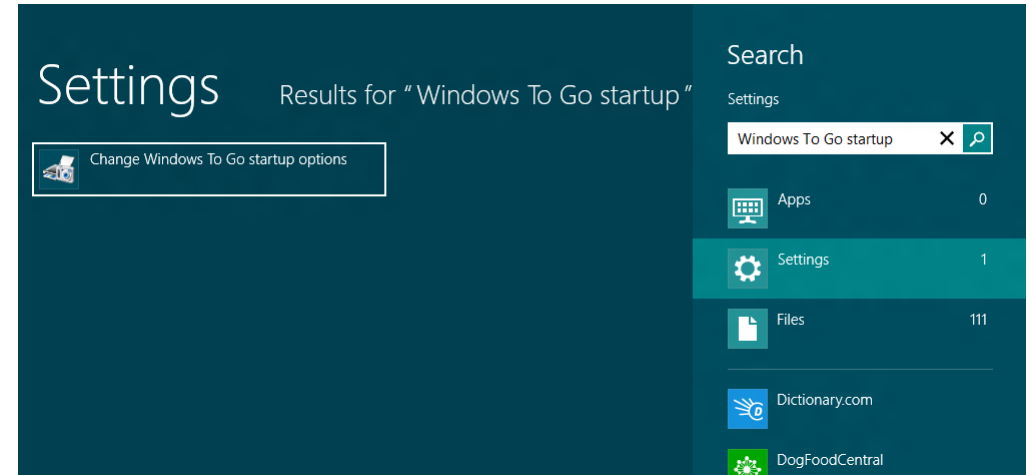
Allows host PCs to automatically boot from USB
Available on Windows 8 and Windows 8.1 hosts

2 Easy Steps in Windows 8 / Windows 8.1

Search for "Windows To Go Startup options"
Select "Yes"

Not Running Windows 8 / Windows 8.1

USB boot "hotkeys"
Configure BIOS to boot from USB



Full Fidelity Experience

High performance

Full native hardware access on the host machine

Same peripheral support as Windows 8.1

Touch enabled, mouse and keyboard aware

Windows 8: New Windows apps in the enterprise

Windows Store is **disabled** by default

For users that don't roam, GP can enable the store

Enterprise sideloading of LOB metro-style apps works regardless

Windows 8.1: New Windows apps in the enterprise

Windows Store is **enabled** by default

Enterprise sideloading of LOB metro-style apps continues to work



Easy to Use: Redefine Mobility

Work Across Multiple PCs

On a new PC drivers are installed on first boot
Identifies computer from characteristics of machine firmware
Stores configuration to boot faster on previously used PCs

Work Across system Firmware

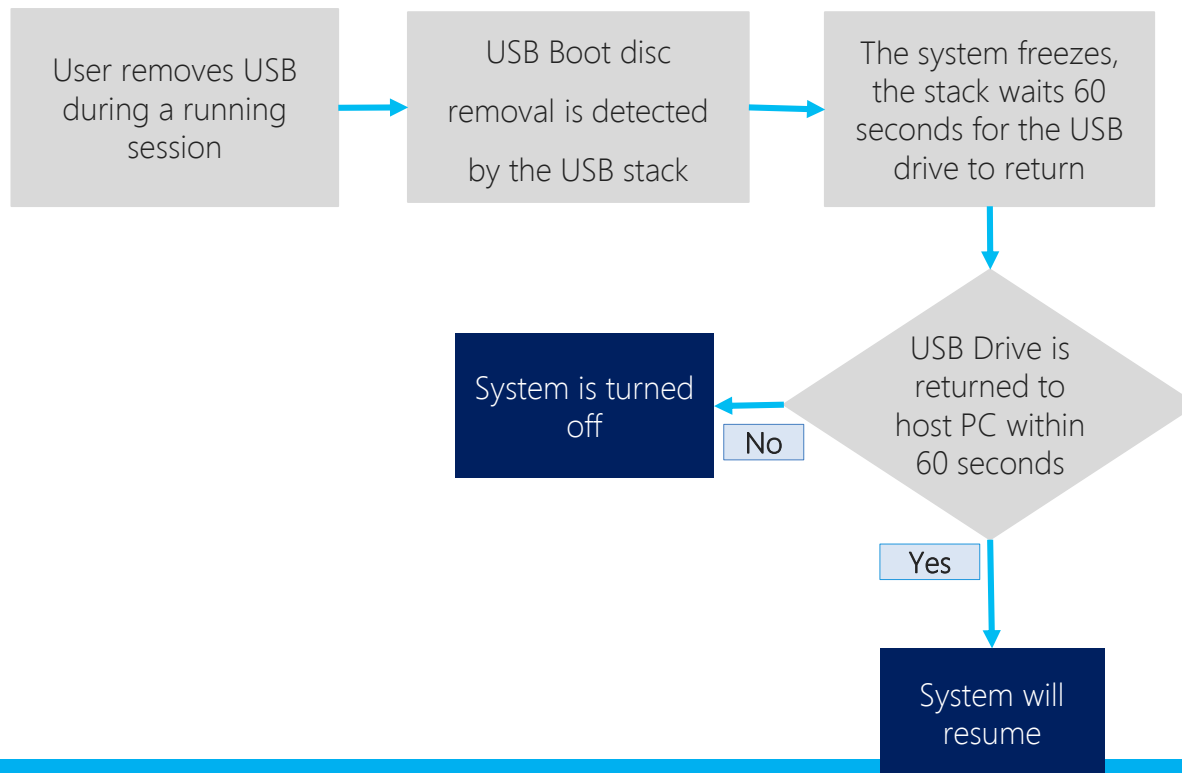
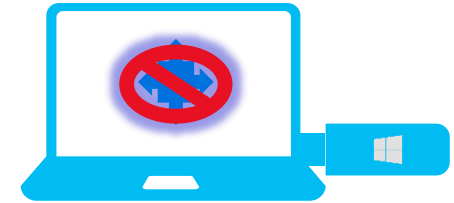
Can be configured to boot on both UEFI and Legacy BIOS
Both sets of boot components are placed on a system partition
Doesn't solve architecture incompatibility



Easy To Use: Resilient to unintended removal

Resilient to unintended removal from host device

- Resumes workspace when USB is put back on within 60 seconds
- Protects data by enforcing system shut down after 60 seconds



Differences Between Windows To Go and Windows

Windows Recovery

Windows Recovery environment is not available
Refresh or Reset your PC is not available

Special Considerations

Hibernate is disabled by default
Don't insert the Windows To Go drive into a running PC
Always shut down Windows and wait for shutdown to complete before removing a Windows To Go drive
Supported on PCs certified for use with Windows 7, 8, and 8.1 regardless of the OS on the machine









Windows To Go Certified Drives

Why is the use of a certified drive important?

- Certified drives are optimized to meet the necessary requirements for booting and running Windows from a USB drive:
 - Built for high random read / write speeds
 - Support thousands of random access I/O per second
 - Provide wear-leveling features improving drive longevity
 - Tuned to ensure they boot and run on hardware certified for use with Windows 7, Windows 8, and Windows 8.1
- Only certified and optimized drives are supported

Windows To Go Certified Drives

Optimized for booting and running Windows 8 and Windows 8.1 Enterprise on hardware certified for use with Windows 7 or higher Windows operating systems.

Manufacturer	Storage size		Manufacturer	Storage size	
Kingston® DataTraveler® Workspace www.kingston.com/wtg	32, 64, 128 GB		Super Talent RC4 www.supertalent.com/wtg	32, 64, 128, 256 GB	
Imation IronKey® Workspace W300 www.imation.com/wtg	32, 64, 128 GB		SPYRUS Portable Workplace™ www.spyruswtg.com	32, 64, 128 GB	
Imation IronKey® Workspace W500 www.imation.com/wtg	32, 64, 128 GB		SPYRUS Secure Portable Workplace™ www.spyruswtg.com	32, 64, 128 GB	
Super Talent Express RC8 www.supertalent.com/wtg	32, 64, 128 GB		WD My Passport Enterprise www.wd.com/wtg	500 GB	

*Microsoft only supports certified drives.

Evaluation: Self Provision with the Creator Tool

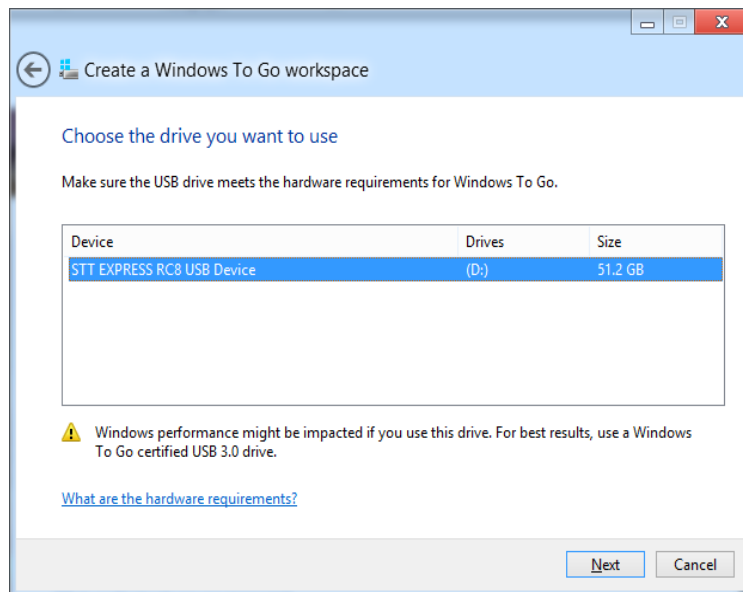
Windows To Go Creator in Windows 8.1 Enterprise

Provision single drive with an Enterprise Image only

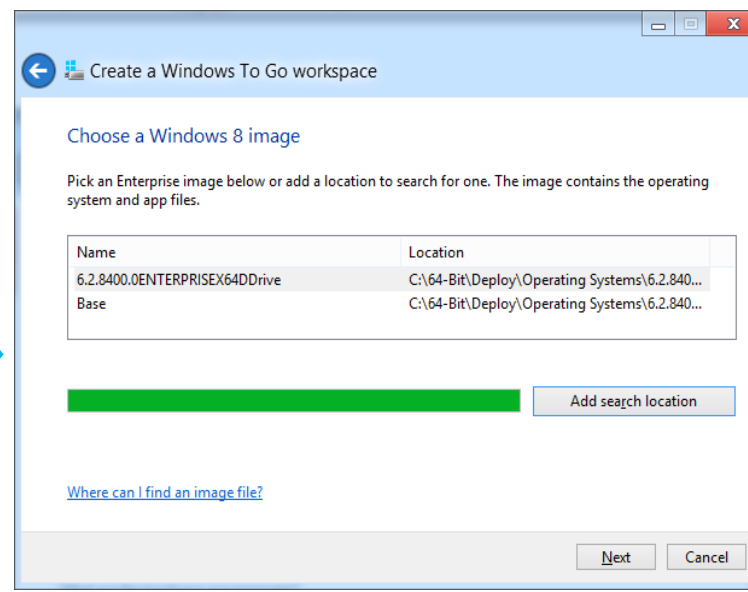
Need admin access

Can be custom WIM or pointed at media

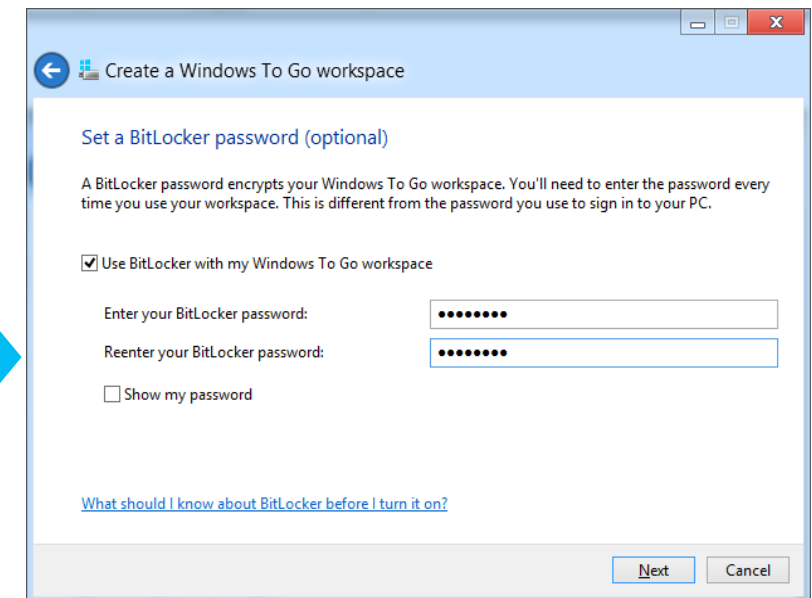
Can enable BitLocker



Select Drive



Select Image



Enable BitLocker

Deployment

Deployment Scenarios

IT Provisioning for central deployment

IT scripts the creation of drives

Users pick up Windows To Go stick from central location

Users boot at work to join domain and enable BitLocker

Windows To Go is ready to use

User Self-Provisioning

System Center 2012 Configuration Manager SP1

System Center 2012 R2 Configuration Manager



IT Provisioning for Central Deployment

IT Admin Experience

Uses PowerShell scripts to provision from Windows 8.1

Provision from Windows 7 with cmd scripts

Can use same tools and image for laptops and Windows To Go

Advanced options like BitLocker at deployment time or Offline Domain Join

(Standard) User Experience

User receives device from IT admin

First boot of the device may occur at home if DirectAccess and Offline Domain Join is utilized

Run Windows To Go device for necessary scenarios

Duplication: IT Provisioning

USB Duplicator

Specialized USB duplication hardware

All drives are identical - user specialization occurs as separate step

Certified drive partners offer duplication services

PowerShell + USB Hub

Use PowerShell's multiple process capabilities

Parallel provisioning of all drives attached to a machine

Allows for unique drive creation (e.g. using Offline Domain Join)

<http://blogs.technet.com/b/deploymentguys/archive/2013/02/27/create-windows-to-go-drives-in-a-simple-factory-mode.aspx>

Deployment: User Self Provisioning

System Center Configuration Manager

IT Admin Experience

- Uses existing Windows 8.1 deployment model for Windows To Go
- Creates prestaged media
- Creates a package with self service tool (provided)
- Deploys the Windows To Go package to the appropriate users

(Standard) User Experience

- Browse the ConfigMgr Application Catalog
- Receives a UI that walks through basic inputs
- Reboots on CorpNet and completes the provisioning process

Manageability

Configure user and system settings with Group Policy

Group Policies introduced specific to Windows To Go

- Power Policy (hibernate and sleep)

- Store Policy

- Windows To Go startup options



System Center Configuration Manager

Inventory software and hardware

Deploy applications and software updates

Settings compliance

System Center 2012 Configuration Manager SP1 for Windows 8 only deployments

System Center Configuration Manager R2 for Windows 8 / 8.1 deployments

How Windows To Go works: Putting it all together

IT

User

Create & Deploy



System Center / Creator Tool

Manage



Management Tools
System Center

Activate



Microsoft
License Activation



Certified
USB Drive



Home



Office



Branch

Work
Across

Boot from managed and
unmanaged PCs

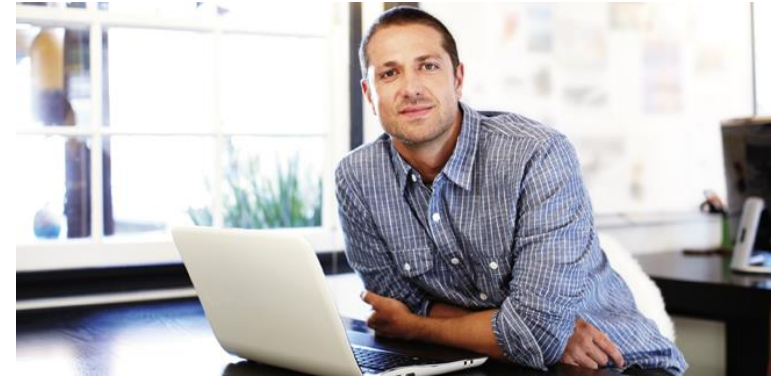
Summary



Provides more Mobility



Easy To Use



Secure & Manageable

Luettaavaa

Web Application Proxy Overview

<http://technet.microsoft.com/en-us/library/dn280944.aspx>

Publishing Internal Applications using Web Application Proxy

<http://technet.microsoft.com/en-us/library/dn383650.aspx>

Secure Anywhere Access to Corporate Resources Such as Windows Server Work Folders Using ADFS

<http://channel9.msdn.com/Events/TechEd/NorthAmerica/2013/WCA-B334#fbid=4qEWnS4oTYO>

Overview: Connect to Applications and Services from Anywhere with Web Application Proxy

<http://technet.microsoft.com/en-us/library/dn280942.aspx>

Overview: Manage Risk with Multi-Factor Access Control

<http://technet.microsoft.com/en-us/library/dn280937.aspx>

Announcing General Availability of Windows Azure Multi-Factor Authentication

<http://blogs.msdn.com/b/windowsazure/archive/2013/09/26/announcing-general-availability-of-windows-azure-multi-factor-authentication.aspx>

Luettavaa

Work Folders

<http://technet.microsoft.com/en-us/library/dn265974.aspx>

Use Exchange ActiveSync Policies for Device Management

<http://technet.microsoft.com/en-us/library/dn282277.aspx>

What's New in Remote Desktop Services in Windows Server 2012 R2

<http://technet.microsoft.com/en-us/library/dn283323.aspx>

Microsoft Remote Desktop –appsit Androidille, iOS:lle sekä Mac OS X:lle

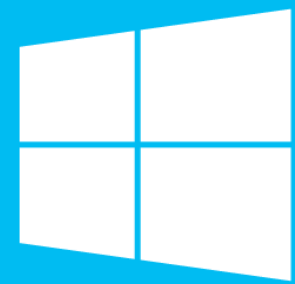
Android: <https://play.google.com/store/apps/details?id=com.microsoft.rdc.android&hl=fi>

iOS: <https://itunes.apple.com/fi/app/id714464092?mt=8&affId=2064962>

Mac OS X: <https://itunes.apple.com/us/app/microsoft-remote-desktop/id715768417?mt=12>

Windows To Go -PowerShell -skripti deploymenttiin

<http://blogs.technet.com/b/deploymentguys/archive/2013/02/27/create-windows-to-go-drives-in-a-simple-factory-mode.aspx>



Windows