

MaaS360[®]

by Fiberlink, an IBM company

MDM Portal

IBM MaaS360 | With Watson

Cerca dispositivi, utenti, app o documenti

HOME DISPOSITIVI UTENTI SICUREZZA APP DOCUMENTI SPESA REPORT CONFIGURA

Il mio centro avvisi

Ultima analisi: mercoledì 11 luglio 2018 7.16.38 EDT

0 Nessun codice di accesso	5 Out of Compliance	3 Config errors
0 Training Devices	13 Android Devices	6 Active Today
19 Missing Patch	0 App rischiose	0 High Data Usage
0 Approvazione in sospeso	13 Malware Detected	42 Devices older than 90 days
0 Roaming	1 Drive Encryption	81 Jailbroken / Rooted

Meno

Dispositivi +
110

Utenti +
1014

App
779

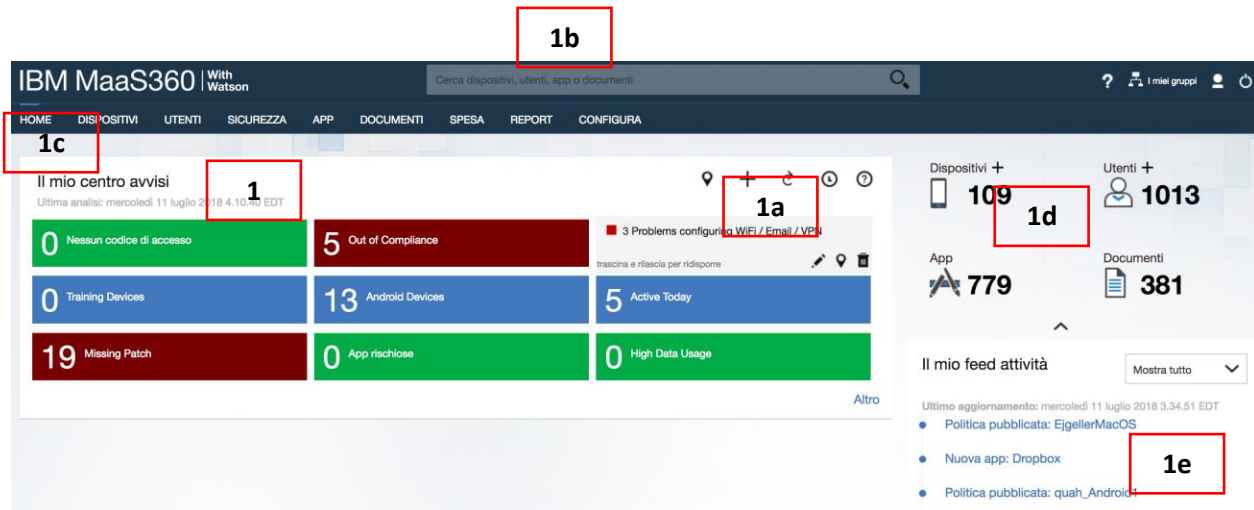
Documenti
381

Il mio feed attività

Mostra tutto

Ultimo aggiornamento: mercoledì 11 luglio 2018 6.27.10 EDT

- Nuovo dispositivo: iPad
- Nuovo utente: ayman.hofi-demo
- Politica pubblicata: EgellerMacOS
- Nuova app: Dropbox
- Politica pubblicata: quah_Android1
- Violazione di una regola per: Posizione
- Violazione della regola cancellata per: Posizione
- Violazione di una regola per: Posizione



Iniziamo con la descrizione della home page e le sue funzionalità.

I punti di seguito riportati indicano:

1. Alert Center.

- a. Nell'Alert Center è possibile aggiungere / modificare / eliminare gli avvisi in base alle proprie esigenze di conformità
- b. Gli avvisi rossi mostrano elementi che violano le politiche impostate
- c. Gli avvisi blu mostrano informazioni istantanee
- d. Gli avvisi verdi mostrano la conformità rispetto alle politiche impostate

(1a.) Utilizzando le icone disponibili in questa area è possibile:

- Ottenere una informazione istantanea di tutte le posizioni del dispositivo
- Aggiungere un nuovo avviso
- Aggiornare le informazioni nel centro avvisi
- Visualizzare la cronologia del centro avvisi

(1b.) Utilizzando la barra di ricerca è possibile cercare facilmente dispositivi, utenti, app e Documenti. Durante la ricerca di utenti, non vengono visualizzate solo le informazioni aggiornate sull'utente, ma anche tutti i dispositivi che sono riconducibili a queste informazioni.

(1c.) La parte superiore dello schermo consente di accedere rapidamente a tutte le principali funzioni di portale. Dispositivi, utenti, impostazioni di sicurezza, app, documenti, gestione delle spese, report e configurazione

(1d.) Appena sotto quello a destra puoi ottenere un'istantanea del tuo ambiente.

Questa area mostra:

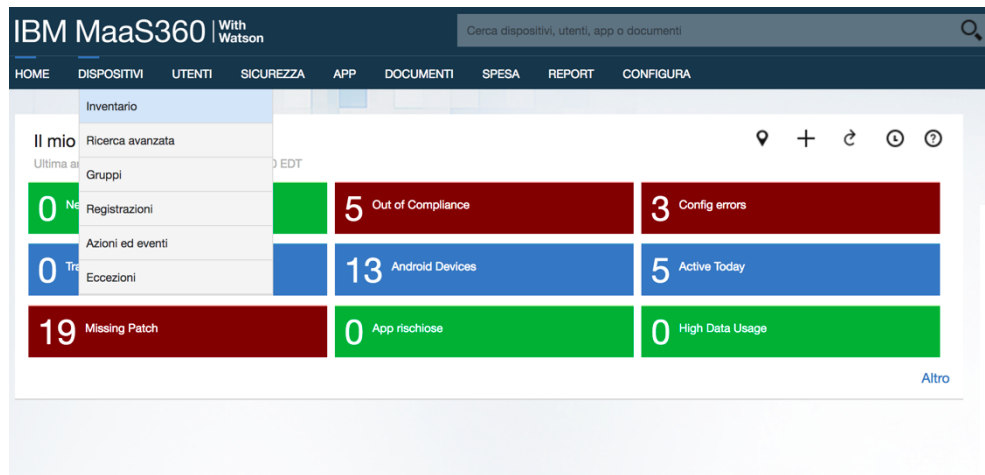
- il numero di dispositivi registrati nel portale
- Il numero di utenti nel portale
- Il numero di app in uso

Il numero di documenti che sono stati caricati

(1e.) La parte in basso a destra dello schermo è il tuo feed di attività.

Questo è il cruscotto di riferimento per avere sotto controllo la conformità alle policy impostate. Registra tutte le azioni intraprese nel portale. (1) (1a.) (1b). (1c).

INVENTARIO DISPOSITIVI



Fare clic sulla voce di menu "Dispositivi", e successivamente selezionare il menu "Inventario".

Apparirà la seguente schermata

The screenshot shows the 'Inventario dispositivo' screen with a table of devices. The table has columns for device name, user, platform, model, system, installation date, last report, status, and email address. The devices listed are:

Nome dispositivo	Nome utente	Piattafo...	Modello	Sistema ...	Data di insta...	Ultimo report	Casella di ...	Indirizzo e...	Stato ge...
ssouder-SM-T710	ssouder	Android	SM-T710	Android 7.0 (NR D90M)	10/09/2017 12:32 EDT	07/11/2018 05:02 EDT	No	scott_souder@us.ibm.com	Registrato
Dan's iPad Air 2	dpaquette	iOS	iPad Air 2	iOS 11	06/02/2015 10:19 EDT	07/11/2018 04:12 EDT	No	dpaquette@instantmdm5.com	Registrato
jpaschal-SM-T819		Android	SM-T819	Android 7.0 (NR D90M)	12/19/2017 05:12 EST	07/11/2018 02:42 EDT	No		Registrato
Martin's iPhone	martintest	iOS	iPhone 8	iOS 11	04/03/2018 15:47 EDT	07/11/2018 02:28 EDT	No	hendrik.jansevanrensburg@gmail.com	Registrato
mranera-PRA-LX1	mranera	Android	PRA-LX1	Android 7.0 (HUAWEIPRA-LX1)	10/25/2017 13:58 EDT	07/11/2018 01:40 EDT	Gestito da ActiveSync	manuel_ranera@es.ibm.com	Registrato
imbellar-SM-G950F	imbellar	Android	SM-G950F	Android 8.0.0 (R16NW)	09/18/2017 01:14 EDT	07/11/2018 00:31 EDT	No	imbellar@in.ibm.com	Registrato
Khaled's iPad	cidemo	iOS	iPad Air 2	iOS 11	03/19/2017 03:47 EDT	07/10/2018 21:16 EDT	Gestito da ActiveSync	cidemo@instantmdm5.com	Registrato

Ogni riga visualizza il nome del dispositivo, nome utente, piattaforma, modello, sistema operativo, data installazione, ultimo report, indirizzo email, stato.

Facendo clic su un tipo di dispositivo attualmente utilizzato dal prospetto apparirà la seguente schermata

IBM MaaS360

With Watson

Cerca dispositivi, utenti, app o documenti

?

1 mio gruppo

HOME

DISPOSITIVI

UTENTI

SICUREZZA

APP

DOCUMENTI

SPESA

REPORT

CONFIGURA

←

Dan's iPad Air 2

Riepilogo

Localizza

Messaggio

Vibrazione

Altro

Inventario hardware

Nome utente	dpaquette	Indirizzo email	dpaquette@instantmdm5.com
Sistema operativo	iOS 11	Produttore	Apple
Modello	iPad Air 2 (MH182LL)	IMEI/MEID	-
ID dispositivo	AppIDMRNR3L1G5W0	Proprietà	Proprietà dipendenti
Modalità di registrazione del dispositivo	Manuale	Convertito da non DEP a DEP	No/NA

WorkPlace e sicurezza

Stato gestito	Registrato	Politica applicata	MDM: Default iOS MDM Policy (9) WorkPlace Persona: ManuelPolicies (83)
Ultimo report	07/11/2018 04:12 EDT(Raggiungibile)	Con jailbreak/root	No
Impostazioni non riuscite	No	Stato cancellazione selettiva	Non applicato
Livello di codifica	A livello di blocco e a livello di file	Stato codice di accesso	MDM:Conforme WorkPlace: Non abilitato
Stato conformità politica	Non conforme	Stato conformità regole	-
Motivi non conformi	Restricted App detected: Facebook	Nome insieme di regole	-

Informazioni sulla rete

Numero di telefono	Non disponibile	ICCID	Non disponibile
Roaming	Non abilitato	Roaming dei dati internazionale	Non abilitato

Cookie Preferences

Fare attenzione alla sezione Workplace e sicurezza

In particolare: Stato Jailbroken
Livelli di crittografia
Politica applicata

Le "policy" o politiche controllano le restrizioni e le configurazioni per il dispositivo.

Alcuni esempi sono: Blocco della fotocamera, Blocco l'app store, pushing down dell'impostazione Email o Impostazioni Wi-Fi

Successivamente cliccando sul Pulsante di riepilogo a discesa, si potrà accedere a Hardware Inventory (1a) per ottenere la schermata (1b)

Hardware Inventory (1a)

Inventario hardware	
Nome utente	dpaquette@instantmdm5.com
Sistema operativo	iOS 11
Modello	iPad Air 2 (MH182LL)
ID dispositivo	DMRN3L1G5W0
Modalità di registrazione del	Manuale
WorkPlace e sicurezza	
Stato gestito	Registrato ✓
Ultimo report	11/2018 04:12 EDT (Raggiungibile) ✓
Impostazioni non riuscite	✓
Livello di codifica	Vello di blocco e a livello di file ✓
Stato conformità politica	Non conforme 1
Motivi non conformi	Restricted App detected: Facebook
Informazioni sulla rete	
Numero di telefono	Non disponibile
ICCID	Non disponibile

Schermata (1b)

Hardware e sistema operativo	
Produttore	Apple
Modello	iPad Air 2 (MH182LL)
Numero di serie piattaforma	DMRN3L1G5W0
UDID	02cc826ac8e5d6cf8bcaac4cb92f8616e175b132
Versione firmware modem	Non disponibile
Data di installazione	06/02/2015 10:19 EDT
Storage interno totale	56.57 GB
Storage interno disponibile	25.97 GB
Dati applicazione	3.51 GB
Livello della batteria	67.0 %
Dettagli del sistema operativo	
Sistema operativo	iOS 11
Versione sistema operativo	11.4 (15F79)
Versione kernel	-
Livello API	5
Versione banda base	-
Numero build	-
ID agent ActiveSync	CKM2OQ2QP5057CJH5D6LPV6JVG
Aggiornamenti disponibili	SI - iOS 11.4.1

Insieme all'infrastruttura di base del dispositivo si possono inserire attributi personalizzati. Questi possono essere utili ad esempio per:

- Gestione degli asset - Informazioni sulla garanzia / ordini di acquisto
- Esigenze dipartimentali - IT / finanza / vendite / ecc.

È possibile raggruppare i dispositivi in base a queste categorie personalizzate ed eseguire azioni su questi gruppi, come ad esempio

Distribuisce app e documenti / Modifica criteri per gruppi / Cambia gruppi di regole / Invia messaggi

Informazioni sulla posizione

Facendo clic su “Informazioni sulla posizione” si possono visualizzare le seguenti informazioni (1c.)

IBM MaaS360 | With Watson

Cerca dispositivi, utenti, app o documenti

HOME DISPOSITIVI UTENTI SICUREZZA APP DOCUMENTI SPESA REPORT CONFIGURA

← Dan's iPad Air 2 Hardware e sistema operativo Localizza Messaggio Vibrazione Altro

Inventario hardware

Prodotto	Modello	iPad Air 2 (MH182LL)
Numero di serie piattaforma	UDID	02cc826ac8e5d6cfd8ccac4cb9219616e175b132
Versione firmware modem	Data di installazione	06/02/2015 10:19 EDT
Storage interno totale	Storage interno disponibile	25.97 GB
Dati applicazione	Informazioni sulla posizione	1 GB
	Livello della batteria	67.0 %

Dettagli del sistema operativo

Sistema operativo	Distribuzioni app	11	Versione sistema operativo	11.4 (15F79)
Versione kernel	Documenti scaricati		Livello API	5
Versione banda base	Certificati		Numero build	-
ID agent ActiveSync	Utilizzo dei dati mobili	M2OQ2QP5057CJH5D6LPV6JVG	Aggiornamenti disponibili	SI - iOS 11.4.1

Cronologia del browser (visitata)

Cronologia del browser (bloccata)

Gruppi

Attributi personalizzati

IBM MaaS360 | With Watson

Cerca dispositivi, utenti, app o documenti

HOME DISPOSITIVI UTENTI SICUREZZA APP DOCUMENTI SPESA REPORT CONFIGURA

← Dan's iPad Air 2 Informazioni sulla posizione Localizza Messaggio Vibrazione Altro

Cronologia posizioni Abilitato. Disabilita su tutti i dispositivi

Utilizzo del servizio di localizzazione: Abilitato

Trova il mio dispositivo: Abilitato

Indirizzo posizione	Ora
12118 Woodbend Dr, Matthews, NC 28105	12/14/2017 23:49 EST

Passa diretta... CSV Esporta

Indirizzo: 12118 Woodbend Dr, Matthews, NC 28105
Data della posizione: 12/14/2017 23:49 EST
Stato di registrazione: Checked-In
Posizione di registrazione: Dan Home Arkfree

© 2018 HERE, © 2018 Microsoft Corporation Terms

Smartphone : Segar's iPhone

Location Information

Actions

Username

Last Reported

rsegar (rsegar@maas360dz.com)

01/28/2014 19:55 UTC

IMEI/MEID

Managed Status

990002728332972

Enrolled

ActiveSync Managed

Location Information

Location History: Enabled. [Disable](#) on all devices.

Use of Location Services: Disabled.

Find My Device: Disabled

Filter Locations by Date: Last 7 days 1

Search:

Export

1.	01/28/2014 19:44 UTC	Checked-In: 1767 Sentry Pkwy W, Blue Bell, PA 19422
2.	01/28/2014 18:54 UTC	Checked-In: 1769 Sentry Pkwy W, Blue Bell, PA 19422
3.	01/28/2014 18:35 UTC	Checked-In: 1769 Sentry Pkwy W, Blue Bell, PA 19422
4.	01/28/2014 18:19 UTC	Checked-In: 1769 Sentry Pkwy W, Blue Bell, PA 19422
5.	01/28/2014 17:59 UTC	Checked-In: 1769 Sentry Pkwy W, Blue Bell, PA 19422
6.	01/28/2014 17:37 UTC	Checked-In: 1769 Sentry Pkwy W, Blue Bell, PA 19422
7.	01/28/2014 17:24 UTC	Checked-In: 1787 Dekalb Pike, Blue Bell, PA 19422
8.	01/28/2014 15:19 UTC	Checked-In: 1769 Sentry Pkwy W, Blue Bell, PA 19422
9.	01/28/2014 12:06 UTC	Checked-In: 1773 Sentry Pkwy W, Blue Bell, PA 19422

Questa funzione può essere disattivata per motivi di privacy

Software installato

Cliccando su App installate si possono visualizzare le seguenti informazioni:

The screenshot shows the IBM MaaS360 interface with a search bar at the top. The navigation bar includes links for HOME, DISPOSITIVI, UTENTI, SICUREZZA, APP, DOCUMENTI, SPESA, REPORT, and CONFIGURA. The main content area displays a list of devices, with 'Dan's iPad Air 2' selected. A dropdown menu is open under the 'Riepilogo' tab, showing various categories of information available for this device, including 'App installate'.

Nome utente	Indirizzo email
Sistema operativo	Produttore
Modello	IMEI/MEID
ID dispositivo	Proprietà
Modalità di registrazione del	Convertito da non DEP a DEP
WorkPlace e sicurezza	
Stato gestito	Politica applicata
Ultimo report	Con jailbreak/root
Impostazioni non riuscite	Stato cancellazione selettiva
Livello di codifica	Stato codice di accesso
Stato conformità politica	Stato conformità regole
Motivi non conformi	Nome insieme di regole
Informazioni sulla rete	
Numero di telefono	ICCID

The screenshot shows the IBM MaaS360 interface with a search bar at the top. The navigation bar includes links for HOME, DISPOSITIVI, UTENTI, SICUREZZA, APP, DOCUMENTI, SPESA, REPORT, and CONFIGURA. The main content area displays a list of devices, with 'Dan's iPad Air 2' selected. The 'App installate' tab is active, showing a table of installed applications.

Nome applica...	ID app	Versione com...	Dimensioni ap...	Dimensioni da...	Gestito	Origine app	Stato di confo...	Azione	Visualizza classifi...
Dr. WiFi	com.trendmicro.consum	2.1.2	35.7	4.07	No	iTunes			
AE Platinum	com.channel4.aesplatinu	1.0.2	253.31	93.11	No	iTunes			
AT Online 2	com.tradegame.airtycoo	1.7.3	220.9	3.75	No	iTunes			
Absolute RC Helicopter	com.rcflightair.cvhell1	3.3.3	93.22	49.29	No	iTunes			
Air Cavalry	com.helicopter.helicopt	3.3	1057.07	3.31	No	iTunes			
AirTycoon2	com.tradegame.airtycoo	1.6.0	130.14	5.07	No	iTunes			
Airlines Manager	com.Playtion.AirlinesMa	2.8.11	135.16	209.93	No	iTunes			
Amazon	com.amazon.Amazon	11.12.0	78.29	88.89	No	iTunes			
Anywhere	com.dishnetwork.DISH-i	7.15	80.71	2.67	No	iTunes			
Apple Store	com.apple.store.Jolly	500000	42.48	0.11	No	iTunes			

Ovvero, nome applicazione / ID applicazione / versione / dimensione, origine e altri attributi (1a.)
MDM può limitare l'accesso alle applicazioni.

Cronologia

La Cronologia Fornisce una traccia di controllo utilizzata per monitorare e tenere traccia delle azioni intraprese nel portale.

Queste informazioni possono essere esportate in formati CSV o Excel.

Un portale può avere più amministratori con diversi ruoli nell'organizzazione.

IBM MaaS360

With Watson

Cerca dispositivi, utenti, app o documenti

HOME

DISPOSITIVI

UTENTI

SICUREZZA

APP

DOCUMENTI

SPESA

REPORT

CONFIGURA

Nome utente		iquette	Indirizzo email
Sistema operativo	Sicurezza e conformità	11	Produttore
Modello	Gestione minacce	d Air 2 (MH182LL)	IMEI/MEID
ID dispositivo	Informazioni sulla rete	0DMRNR3L1G5W0	Proprietà
Modalità di registrazione del	Informazioni sulla posizione	nuale	Convertito da non DEP a DEP
WorkPlace e sicurezza			
Stato gestito	Distribuzioni app	registrato	Politica applicata
	Documenti scaricati		
Ultimo report		11/2018 04:12 EDT(Raggiungibile)	Con jailbreak/root
Impostazioni non riuscite	Certificati		Stato cancellazione selettiva
Livello di codifica	Utilizzo dei dati mobili	vello di blocco e a livello di file	Stato codice di accesso
	Cronologia del browser (visitata)		
Stato conformità politica	Cronologia del browser (bloccata)	n conforme	Stato conformità regole
Motivi non conformi		stricted App detected: Facebook	Nome insieme di regole
	Gruppi		
Informazioni sulla rete			
Numero di telefono	Cronologia	n disponibile	ICCID
Roaming		n abilitato	Roaming dei dati internazionale
Gestore domestico	Servizi installati	non disponibile	Tipo di rete attuale

IBM MaaS360

With Watson

Cerca dispositivi, utenti, app o documenti

Azioni

Last Know Location: Coperto nella panoramica del dispositivo

Send Message: il messaggio viene ricevuto sull'app MaaS360 sul dispositivo (e-mail in basso, avvisa il tuo staff)

Buzz Device- Il dispositivo emette un suono di sirena

Lock Device - Blocca il dispositivo sulla sua schermata iniziale così che l'utente deve reinserire la propria password o pin (iOS7- È possibile inviare un messaggio con un # per chiamare se il dispositivo è perso o rubato)

Reset the Device Passcode: iOS cancella il pin del dispositivo, l'utente può inserirne uno nuovo Android- Lets admin cambia il pin

Selective Wipe: rimuovi le informazioni aziendali senza interagire con i dati personali. Qualunque cosa l'app MaaS360 spinta verso il basso viene rimossa. E-mail / Wifi / VPN / Documenti / App (Revoca, l'impostazione può essere ripristinata dall'amministratore)

Wipe: Ripristina completamente il dispositivo alle impostazioni di fabbrica

L'amministratore eo l'utente possono essere avvisati quando vengono avviati. Richiede PW di amministrazione per iniziare.

Suggerimento: se un dispositivo è offline quando viene eseguita un'azione, l'azione è in sospeso fino a quando il dispositivo non verrà acceso.

BM MaaS360 With Watson

Cerca dispositivo, utenti, app o documenti

HOME DISPOSITIVI UTENTI SICUREZZA APP DOCUMENTI SPESA REPORT CONFIGURA

← Dan's iPad Air 2 Riepilogo

Localizza Messaggio Vibrazione Altro

Inventario hardware

Nome utente	dpaquette	Indirizzo email	dpaquette@instantr
Sistema operativo	iOS 11	Produttore	Apple
Modello	iPad Air 2 (MH182LL)	IMEI/MEID	-
ID dispositivo	AppIDMRN93L1G5W0	Proprietà	Proprietà dipendenti
Modalità di registrazione del dispositivo	Manuale	Convertito da non DEP a DEP	No/NA

WorkPlace e sicurezza

Stato gestito	Registrato	Politica applicata	MDM: Default iOS / Workplace Personal
Ultimo report	07/11/2018 04:12 EDT(Raggiungibile)	Con jailbreak/root	No
Impostazioni non riuscite	No	Stato cancellazione selettiva	Non applicato
Livello di codifica	A livello di blocco e a livello di file	Stato codice di accesso	MDM: Conforme / Workplace: Non abilitato
Stato conformità politica	Non conforme	Stato conformità regole	-
Motivi non conformi	Restricted App detected: Facebook	Nome insieme di regole	-

Informazioni sulla rete

Blocca
Reimposta codice di accesso
Cancella
Configurazione per la lezione
Modifica politica
Modifica insieme di regole
Modifica piano
Cancellazione selettiva
Rimuovi controllo
Nascondi
Richiedi aggiornamento dati
Avvia supporto remoto

Sicurezza e Politiche

Fare click su "Security" nella parte superiore della pagina e successivamente sulla voce "Politiche".

IBM MaaS360

With Watson

Cerca dispositivi, utenti, app o documenti

HOME DISPOSITIVI UTENTI SICUREZZA APP DOCUMENTI SPESA REPORT CONFIGURA

Politiche

Gestione delle politiche

Politiche

i

Per ulteriori informazioni

Gestione patch

utilizzarle in modo efficiente, [fare clic qui](#)

Nome		Stato	Precedenza	Disponibile per
EjgellerMacOS	Patch sistema operativo (Windows)	Publicato	60	All
Visualizza Cronologia Esporta	Patch sistema operativo (Mac)			
Gruppi a cui si applica: Nessuno	Aggiornamenti app (Windows)			
quah_Android1	Aggiornamenti app (Mac)	Publicato	76	All
Visualizza Cronologia Esporta	Ricerca di patch			
Gruppi a cui si applica: [quah_SPS_group]	Aggiornamenti app Windows	Bozza		All
asfgafgrG				
Visualizza Esporta				
testioscwe123		Bozza	526	All
Visualizza Esporta				

Si possono verificare le politiche di default e ad esempio il criterio MDM predefinito di iOS.

IBM MaaS360

With Watson

Cerca dispositivi, utenti, app o documenti

?

1 miei gruppi

HOME DISPOSITIVI UTENTI SICUREZZA APP DOCUMENTI SPESA REPORT CONFIGURA

Gruppi a cui si applica: Nessuno

test_toyota	Bozza	340	All		06/01/2018 04:03 EDT
Visualizza Esporta					
test_dg	Bozza		All		05/31/2018 09:46 EDT
Visualizza Esporta					
ejgellerpersona	In attesa di pubblicazione	63	All		05/30/2018 14:21 EDT
Gruppi a cui si applica: [Ejgeller Win10 devi...					05/10/2017 21:33 EDT
Quah Intune MAM iOS	In attesa di pubblicazione		All		05/27/2018 23:33 EDT
Visualizza Cronologia Esporta					04/08/2018 21:11 EDT
quah_IOS1	Publicato	102	All		05/25/2018 02:54 EDT
Visualizza Cronologia Esporta					05/25/2018 02:54 EDT
Gruppi a cui si applica: [quah_SPS_group]					
IOS MDM Policy	In attesa di pubblicazione	42	All		05/24/2018 13:11 EDT
Visualizza Cronologia Esporta					11/08/2017 15:05 EST
Gruppi a cui si applica: [Alvin's Group.grp_t...					
poli cogni	Bozza	522	All		05/24/2018 11:51 EDT
Visualizza Esporta					
Gruppi a cui si applica: Nessuno					
GDPR 2	Bozza	374	All		05/24/2018 09:41 EDT
Visualizza Esporta					
Gruppi a cui si applica: Nessuno					
GDPR					

Seleziona "Workplace" sulla sinistra (Workplace è la posta sicura e parte dell'SPS).

IBM MaaS360

With Watson

Cerca dispositivi, utenti, app o documenti

HOME

DISPOSITIVI

UTENTI

SICUREZZA

APP

DOCUMENTI

SPESA

REPORT

CONFIGURA

←

Default iOS MDM Policy

Ultima pubblicazione: 11/08/2017 15:05 EST [Versione:9] Stato corrente: In attesa di pubblicazione

Impostazioni del dispositivo

Codice di accesso

Restrizioni

Conformità dell'applicazione

ActiveSync

Gestione minacce Trusteer

Wi-Fi

VPN

AirPrint

Account

Impostazioni avanzate

Impostazioni supervisionate

Configura politica codice di accesso

Si

Codice di accesso

Implementa codice di accesso sul dispositivo mobile

Si

Consenti codice di accesso semplice

I valori di codice di accesso che sono delle sequenze di caratteri crescenti, decrescenti o ripetuti (ad es.11111, 123, 654, abc, xyz).

Si

Richiedi caratteri alfanumerici nel codice di accesso (almeno una lettera)

No

Lunghezza minima codice di accesso

Selezionare un numero compreso tra 4 e 16. IOS consiglia di impostare su 6 o superiore.

4

Numero richiesto di caratteri speciali (1-4)

--

Durata massima del codice di accesso (1-730 giorni o vuoto)

La funzione “Codice di Accesso” può forzare una seconda password per accedere a Workplace o Container

IBM MaaS360

With Watson

Cerca dispositivi, utenti, app o documenti

HOME

DISPOSITIVI

UTENTI

SICUREZZA

APP

DOCUMENTI

SPESA

REPORT

CONFIGURA

←

Default iOS MDM Policy

Ultima pubblicazione: 11/08/2017 15:05 EST [Versione:9] Stato corrente: In attesa di pubblicazione

Impostazioni del dispositivo

Codice di accesso

Restrizioni

Conformità dell'applicazione

ActiveSync

Gestione minacce Trusteer

Wi-Fi

VPN

AirPrint

Account

Impostazioni avanzate

Impostazioni supervisionate

Configura politica codice di accesso

Si

Codice di accesso

Implementa codice di accesso sul dispositivo mobile

Si

Consenti codice di accesso semplice

I valori di codice di accesso che sono delle sequenze di caratteri crescenti, decrescenti o ripetuti (ad es.11111, 123, 654, abc, xyz).

Si

Richiedi caratteri alfanumerici nel codice di accesso (almeno una lettera)

No

Lunghezza minima codice di accesso

Selezionare un numero compreso tra 4 e 16. IOS consiglia di impostare su 6 o superiore.

4

Numero richiesto di caratteri speciali (1-4)

--

Durata massima del codice di accesso (1-730 giorni o vuoto)

Impostazioni del dispositivo

The screenshot shows the IBM MaaS360 interface with the 'Default iOS MDM Policy' selected. The left sidebar lists various settings: Impostazioni del dispositivo (selected), Codice di accesso, Restrizioni, Conformità dell'applicazione, ActiveSync, Gestione minacce Trusteer, Wi-Fi, VPN, AirPrint, and Account. The main area displays the 'Codice di accesso' settings, which are currently set to 'Sì' (Yes). The settings include: Configura politica codice di accesso (Sì), Implementa codice di accesso sul dispositivo mobile (Sì), Consenti codice di accesso semplice (Sì), Richiedi caratteri alfanumerici nel codice di accesso (almeno una lettera) (No), Lunghezza minima codice di accesso (4), Numero richiesto di caratteri speciali (1-4) (—), and Durata massima del codice di accesso (1-730 giorni o vuoto).

Password:

è possibile impostare la passcode del dispositivo

L'utente finale può decidere la passcode-Admin definisce i parametri della password

Restrizioni:

utilizzato per limitare la funzionalità del dispositivo (fare una domanda di sondaggio qui per identificare quelli giusti per dimostrare) I più comuni sono: Block App Store, Block Multiplayer gaming Blocca Siri, Blocca FaceTime, Blocca iCloud, Blocca negli acquisti di app.

Applicazione di Conformità:

Black list: mette fuori uso l'utente se non ha installato l'app.

Whitelist: mette fuori uso l'utente se ha installato l'app

App richieste: app obbligatorie da installare

iOS: impossibile forzare la rimozione, ma il dispositivo viene limitato diventando non conforme (le azioni disponibili includono: Pulizia selettiva / Ammin. avvisi / Pulisci dispositivo / Ecc.)

L'app Android-Can Block può essere utilizzata o si può obbligare l'utente a rimuovere l'app

Activesync:

invia email al client nativo su un dispositivo

* Non è sicuro come un contenitore come la posta sicura

Wifi:

Consente di inviare le impostazioni Wi-Fi all'utente finale

* Utile per dare accesso istantaneo alle reti private

* Può essere rimosso selettivamente

VPN:

premere Impostazioni VPN sul dispositivo

Regole di compliance



Cliccare sul menu “Security” e successivamente sulla voce “Compliance Rules” per visualizzare le seguenti informazioni:

The screenshot shows the 'Compliance Rules' page in MaaS360. The top navigation bar includes 'DEVICES', 'USERS', 'SECURITY', 'APPS', 'DOCS', 'EXPENSES', 'REPORTS', and 'SETUP'. The 'SECURITY' tab is selected. The page title is 'Compliance Rules'. There are buttons for 'Add Rule', 'Precedence', 'Disable All', and 'Show All', along with a search bar. Below the buttons is a list of instructions for creating and managing rule sets. The main content is a table with the following columns: 'Rule Set Name', 'Available for', 'Default', 'Status', 'Precedence', '# of Devices', 'Last Updated By', and 'Last Updated On'. The table contains 7 rows of data.

Rule Set Name	Available for	Default	Status	Precedence	# of Devices	Last Updated By	Last Updated On
Test Geo Edit Assign Make Default Audit Delete Groups Applied to: None	All		Active	10	0	mdm_ddecarlo	01/20/2014 19:47 UTC
Test-AD Edit Assign Make Default Audit Delete Groups Applied to: None	All		Active	9	0	mdm_adoble	01/08/2014 19:36 UTC
JR Test Rule Set Edit Assign Make Default Audit Delete Groups Applied to: None	All		Active	8	0	jraymond_1038	12/21/2013 12:49 UTC
Test Ja Edit Assign Audit Delete Groups Applied to: None	Product		Active	7	0	mdm_jallen	12/16/2013 09:51 UTC
Katie compliance rules Edit Assign Make Default Audit Delete Groups Applied to: None	All		Active	6	0	mdm_cschoopy	12/12/2013 15:25 UTC
test12345 Edit Assign Make Default Audit Delete Groups Applied to: None	All		Active	5	0	tanveer_demo	12/10/2013 06:19 UTC

Le regole di compliance consentono la gestione dei dispositivi non conformi.

Le azioni possono essere effettuate immediatamente o dopo un tempo impostato.

Esempi:

- Limita Jailbroken o Rooted
- Limita i dispositivi con app in blacklist
- Limita i dispositivi senza l'appropriato livello di crittografia

I tipi di restrizioni includono

- Avviso all'utente e / o amministratore
- Block - Spegni l'accesso e-mail (Richiede Cloud Extender)
- Selective Wipe
- Change Policy
- Wipe- Completa la pulizia del dispositivo

Update Rule Set "Test Geo"

Basic Settings

Enforcement Rules

Geo-Fencing Rules

Monitoring Rules

Expense Monitoring Rules

Enable Geo-Fencing Rules to enforce location related compliance for mobile devices.

1. Enable Geo-Fencing enforcement to alert, change policy, or take action on devices that exit, or check-out of, approved locations. Locations can be created from SECURITY > Locations.
2. Select the action needed to be taken on devices that go out of compliance. Available actions can vary based on level of e-mail server integration.
3. You can opt to specify an action grace period in hours or days. Grace period will give the user a chance to self-remediate violations, before the selection action is taken.
4. If changing policy based on location, select the appropriate policy to apply when devices exits, or check-out of, defined location.
5. Use the "Alert Administrator" action, if you don't want users to be notified when they check-out of the approved locations but would still want to be made aware of such instances.

Select Geo-Fencing Rule(s)

Enable Geo-Fencing
Enforces the devices to stay checked-in at all times. You need to have defined locations before enabling this rule. You can define new locations from SECURITY > Locations.

☒

Enforcement Action
Alert Administrator

Message (maximum 250 characters)
Enter comments to notify and users.

Si possono intraprendere azioni limitate quando un dispositivo non è in una corretta posizione geografica.

Le posizioni sono definite da SSID Wi-Fi o da un indirizzo fisico all'interno del raggio incluso (configurato in sicurezza e posizioni).

Update Rule Set "Test Geo"

Basic Settings

Enforcement Rules

Geo-Fencing Rules

Monitoring Rules

Expense Monitoring Rules

Enable Expense Monitoring Rules to get real-time alerts for expense management.

1. Expense Monitoring will send alerts to users and administrators when devices exceed defined thresholds of roaming and in-network data usage. Data usage plans can be created via 'Manage Plans'.
2. To enable Expense Monitoring Rule(s), check the option next to the desired rule to enable.
3. Select threshold percentages (of assigned plan) for desired warning notifications.
4. Select alert type to perform when data usage threshold is reached. Alerts can be sent to administrators, or both users and admins.
5. Enter warning message that will be sent to the user when data usage threshold is exceeded.

Select Expense Monitoring Rules

Monitor Roaming Mobile Data Usage
Monitor and notify users and administrators when roaming mobile data usage on the device exceeds defined thresholds.

☒

First Warning Level (%)
Select a value

Actions
☐ Alert User ☐ Alert Administrator

Message (maximum 140 characters)
First Warning Level : You have used %limit% of your monthly roaming mobile data usage limit.

Second Warning Level (%)
Select a value

Actions
☐ Alert User ☐ Alert Administrator

Message (maximum 140 characters)
Second Warning Level : You have used %limit% of your monthly roaming mobile data usage limit.

Final Warning Level (%)
Select a value

Actions
☐ Alert User ☐ Alert Administrator

Message (maximum 140 characters)
Final Warning Level : You have used %limit% of your monthly roaming mobile data usage limit.

Expense Monitoring invia tre livelli di avvisi quando un utente raggiunge determinate soglie di utilizzo.

Solo un carrier può bloccare il servizio.

La tolleranza dati è configurata sotto Expense> Manage Plans.

Catalogo App

MaaS360 può aggiungere app da tutti i principali app store o app aziendali.
(itunes / Google Play / Windows Store)

IBM MaaS360 | With Watson

Cerca dispositivi, utenti, app o documenti

HOME DISPOSITIVI UTENTI SICUREZZA APP DOCUMENTI SPESA REPORT CONFIGURA

Il mio centro avvisi
Ultima analisi: mercoledì 11 luglio 2018 6.05.29 EDT

0 Nessun codice di accesso

0 Training Devices

19 Missing Patch

Catalogo

Bundle

App installate

Attributi app

Package Windows

3 Config errors

13 Android Devices

0 App rischiose

6 Active Today

0 High Data Usage

Altro

Dispositivi + 10

Il mio feed

Ultimo aggiorni

Politica pu

Nuova ap

Politica pu

Violazione

Fare clic o passare il mouse su aggiungi per mostrare la selezione:

IBM MaaS360 | With Watson

Cerca dispositivi, utenti, app o documenti

HOME DISPOSITIVI UTENTI SICUREZZA APP DOCUMENTI SPESA REPORT CONFIGURA

Catalogo delle app

<input type="checkbox"/>	Icon...	Nome	Tipo	Categorie	Numero insta...	Distrib...	Bundle...	Presen...	Approv...	Codici VPP	Ultimo aggiornamento	Versione app
<input type="checkbox"/>		LEGO® Star Wars™: The Force Awakens Visualizza Altro...		Games	inferiore a 10		No	No	No	No	07/10/2018 21:01 EDT	1.4.0
<input type="checkbox"/>		Okta Mobile Visualizza Altro...		Business	inferiore a 10		No	No	No	No	07/10/2018 21:01 EDT	5.18.0
<input type="checkbox"/>		FieldEdge Visualizza Altro...		Business	inferiore a 10		No	No	No	No	07/10/2018 21:01 EDT	1.65.0
<input type="checkbox"/>		Lowe's Home Improvement Visualizza Altro...		Shopping	inferiore a 10		No	No	No	No	07/10/2018 21:01 EDT	4.15.4
<input type="checkbox"/>		Project Color™ The Home Depot Visualizza Altro...		Lifestyle	inferiore a 10		No	No	No	No	07/10/2018 21:01 EDT	1.1.44
<input type="checkbox"/>		The Weather Channel: Forecast Visualizza Altro...		Weather	inferiore a 10		No	No	No	No	07/10/2018 21:01 EDT	9.11
<input type="checkbox"/>		Geotab Drive Visualizza Altro...		Business	inferiore a 10		No	No	No	No	07/10/2018 21:01 EDT	4.0.0
<input type="checkbox"/>		FANDOM for: Star Wars Visualizza Altro...		Reference	inferiore a 10		No	No	No	No	07/10/2018 21:01 EDT	2.9
<input type="checkbox"/>		HCSS TimeClock Visualizza Altro...		Productivity	inferiore a 10		No	No	No	No	07/10/2018 21:01 EDT	3.3
<input type="checkbox"/>		períodico EL TIEMPO Visualizza Altro...		News	inferiore a 10		SI	No	No	No	07/10/2018 21:01 EDT	3.0
<input type="checkbox"/>		Trips by Verizon Connect Visualizza Altro...		Business	inferiore a 10		No	No	No	No	07/10/2018 21:01 EDT	1.3.1

IBM MaaS360 | With Watson

Cerca dispositivi, utenti, app o documenti

HOME DISPOSITIVI UTENTI SICUREZZA APP DOCUMENTI SPESA REPORT CONFIGURA

Catalogo delle app

1 App : Deseleziona tutto

<input checked="" type="checkbox"/>		LEGO® Star Wars™: The Force Awakens Visualizza Altro...		Games	inferiore a 10		No	No	No	No
<input type="checkbox"/>		Okta Mobile Visualizza Altro...		Business	inferiore a 10		No	No	No	No
<input type="checkbox"/>		FieldEdge Visualizza Altro...		Business	inferiore a 10		No	No	No	No

Digitando il nome dell'app nella barra di ricerca in alto a destra della pagina dell'app. si può cliccare su “Distribute” per distribuire l'app ad un individuo, gruppo o dispositivo specifico.

The screenshot shows the IBM MaaS360 interface. The top navigation bar includes 'HOME', 'DISPOSITIVI', 'UTENTI', 'SICUREZZA', 'APP', 'DOCUMENTI', and 'SP'. The main content area is titled 'Catalogo delle app' and displays a table of applications. A search bar at the top right contains the text 'Okta Mobile'. Below the search bar, a dropdown menu shows search results for 'Okta Mobile', including 'Visualizza' and 'Distribuisce' links. The table below the search bar lists applications with columns for 'Icon...', 'Nome', 'Tipo', and 'Catego'. The first two rows are 'LEGO® Star Wars™: The Force Awakens' (Games) and 'Okta Mobile' (Business). The 'Okta Mobile' row is highlighted. To the right of the table, there is a section for 'Okta Mobile' with a search bar and a list of users, including 'drovers(mobileservice@detron.nl)'.

Icon...	Nome	Tipo	Catego
	LEGO® Star Wars™: The Force Awakens Visualizza Altro...		Games
	Okta Mobile Visualizza Altro...		Business

Utenti	App	Ultimo aggiornamento
drovers(mobileservice@detron.nl) Visualizza Mostra dispositivi	Okta Mobile Visualizza Distribuisce	07/10/2018 21:01 EDT
	OPIE Mobile Visualizza Distribuisce	07/10/2018 21:01 EDT
	ServiceTitan Mobile Visualizza Distribuisce	07/10/2018 21:01 EDT

Per le app aziendali si possono caricare il file ipk Apple o il file apk Andriod.

(I file ipk / apk sono file eseguibili simili a un file .exe di Windows e permetteranno di installare l'app sul dispositivo).

Documenti e libreria contenuti

Attraverso il MaaS è possibile caricare e distribuire documenti e file MaaS360 App per gli utenti finali.

IBM MaaS360

With Watson

ServiceTitan Mobile

HOME DISPOSITIVI UTENTI SICUREZZA APP DOCUMENTI SPESA REPORT CONFIGURA

Libreria contenuti: Tutti i documenti

Documento	Disponibi...	Tipo	Dimensioni	Tag	Download	Implementa pas...	Impedisci l'espo...
Users Apri	Tutti			Altri		No	No
Islamet Apri Visualizza	Tutti			Altri		No	No
DMiles Apri Visualizza	Tutti			Altri		No	No

IBM MaaS360

With Watson

Cerca dispositivi, utenti, app o documenti

HOME DISPOSITIVI UTENTI SICUREZZA APP DOCUMENTI SPESA REPORT CONFIGURA

Libreria contenuti: Tutti i documenti

Cancella i filtri Altro

Documento	Disponibi...	Tipo	Dimensioni	Tag	Download	Implementa pas...	Impedisci l'espo...	Ultimo aggiorna...
Users Apri	Tutti			Altri		No	No	06/26/2014 23:43 EDT
Islamet Apri Visualizza	Tutti			Altri		No	No	05/22/2018 02:22 EDT
DMiles Apri Visualizza	Tutti			Altri		No	No	05/22/2018 00:46 EDT
quah_folder Apri Visualizza	Tutti			Altri		No	Si	05/10/2018 07:20 EDT
Groupe 2 docs Apri Visualizza	Tutti			Altri		No	No	02/07/2018 04:15 EST
Groupe 1 docs Apri Visualizza	Tutti			Altri		No	No	02/07/2018 04:14 EST
MaaS360 Apri Visualizza	Tutti			Altri		No	No	02/06/2018 06:12 EST
Manuel's Folder MaaS360 Apri Visualizza	Tutti			Apple IBM		No	No	02/06/2018 06:12 EST

IBM MaaS360

With Watson

Cerca dispositivi, utenti, app o documenti

HOME DISPOSITIVI UTENTI SICUREZZA APP DOCUMENTI SPESA REPORT CONFIGURA

Libreria contenuti: Tutti i documenti

Cancella i filtri Altro

Impostazioni dei documenti

Documento	Disponibi...	Tipo	Dimensioni	Tag	Download	Implementa pas...	Impedisci l'espo...	Ultimo aggiorna...
Users Apri	Tutti			Altri		No	No	06/26/2014 23:43 EDT
Islamet Apri Visualizza	Tutti			Altri		No	No	05/22/2018 02:22 EDT
DMiles Apri Visualizza	Tutti			Altri		No	No	05/22/2018 00:46 EDT
quah_folder Apri Visualizza	Tutti			Altri		No	Si	05/10/2018 07:20 EDT

IBM MaaS360 | With Watson

Cerca dispositivi, utenti, app o documenti

?

I miei gruppi

HOME

DISPOSITIVI

UTENTI

SICUREZZA

APP

DOCUMENTI

SPESA

REPORT

CONFIGURA

← Impostazioni

Salva

Impostazioni di registrazione del

Impostazioni utente

Impostazioni dei documenti

Base

Impostazioni amministratore

Impostazioni della WorkPlace

☐ Implementa password per l'accesso ai documenti
 ☐ Impedisci l'accesso ai dispositivi con jailbreak
 ☐ Limita la visibilità ai documenti dell'utente

Impostazioni di sicurezza

Definire le impostazioni di sicurezza per i documenti. Nota: le impostazioni sono ereditate dalla cartella padre.
 ☐ Impedisci l'esportazione
 ☐ Impedisci funzioni di Taglia/Copia/Incolla

Valori predefiniti per il download dei documenti

Configurare le politiche di download per i documenti.
 ☐ Protetto da password
 ☒ Scarica in automatico
 ☒ Scarica solo tramite Wi-Fi
 ☐ Nascondi anteprima documento nell'app
 ☐ Impedisci l'eliminazione dopo il download

Di seguito la schermata per aggiungere nuovi documenti

IBM MaaS360 | Watson

Cerca dispositivi, utenti, app o documenti

?

I miei gruppi

HOME

DISPOSITIVI

UTENTI

SICUREZZA

APP

DOCUMENTI

SPESA

SCUOLE

REPORT

CONFIGURA

Libreria contenuti: Tutti i documenti

Cancella i filtri

Aggiungi cartella

Aggiungi documenti

Altro ▾

Aggiungi documenti
Tutti i documenti

Disponibile per: Tutti

Seleziona file * Browse Specifica URL
Selezione di più file (fino a 15) supportata. Le cartelle selezionate verranno ignorate.

Nomi dei documenti * Immettere i nomi dei documenti

Tag Immettere tag separate da virgole

Impostazioni di sicurezza
Definire le impostazioni di sicurezza per i documenti selezionati. Il supporto delle politiche varia in base al sistema operativo del dispositivo. Passare il puntatore del mouse sul nome della politica per dei dettagli di supporto aggiuntivi.

<input type="checkbox"/> Impedisci l'esportazione	<input type="checkbox"/> Consenti app nella whitelist
<input type="checkbox"/> Impedisci funzioni di Taglia/Copia/Incolla	<input type="checkbox"/> Impedisci Secure Mail
	<input type="checkbox"/> Ignora restrizioni di WorkPlace

Politiche di download
Configurare le politiche di download per i documenti. Il supporto delle politiche varia in base al sistema operativo del dispositivo. Passare il puntatore del mouse sul nome della politica per dei dettagli di supporto aggiuntivi.

<input type="checkbox"/> Protetto da password	<input checked="" type="checkbox"/> Scarica solo tramite Wi-Fi
<input checked="" type="checkbox"/> Scarica in automatico	<input type="checkbox"/> Impedisci l'eliminazione dopo il download
<input type="checkbox"/> Nascondi anteprima document o nell'app	

Distribuisci a: Nessuno +

Annulla Salva

Funzione Time Bomb

Una volta scelto un utente / gruppo / dispositivo per distribuire il documento puoi impostare una Time Bomb per una data in futuro che rimuoverà il documento dal dispositivo.

Download Policies
Configure download policies for documents. Supported on iOS only

<input checked="" type="checkbox"/> Password Protected	<input checked="" type="checkbox"/> Download only on Wi-Fi
<input checked="" type="checkbox"/> Download Automatically	<input checked="" type="checkbox"/> Restrict Delete after Download
<input checked="" type="checkbox"/> Hide Doc Preview in App	

Distribute to

Device ▼ Enter device name or user ⊖ ⊕

Enter expiration date 📅 ✕

Cancel Save

Reports Inventario hardware

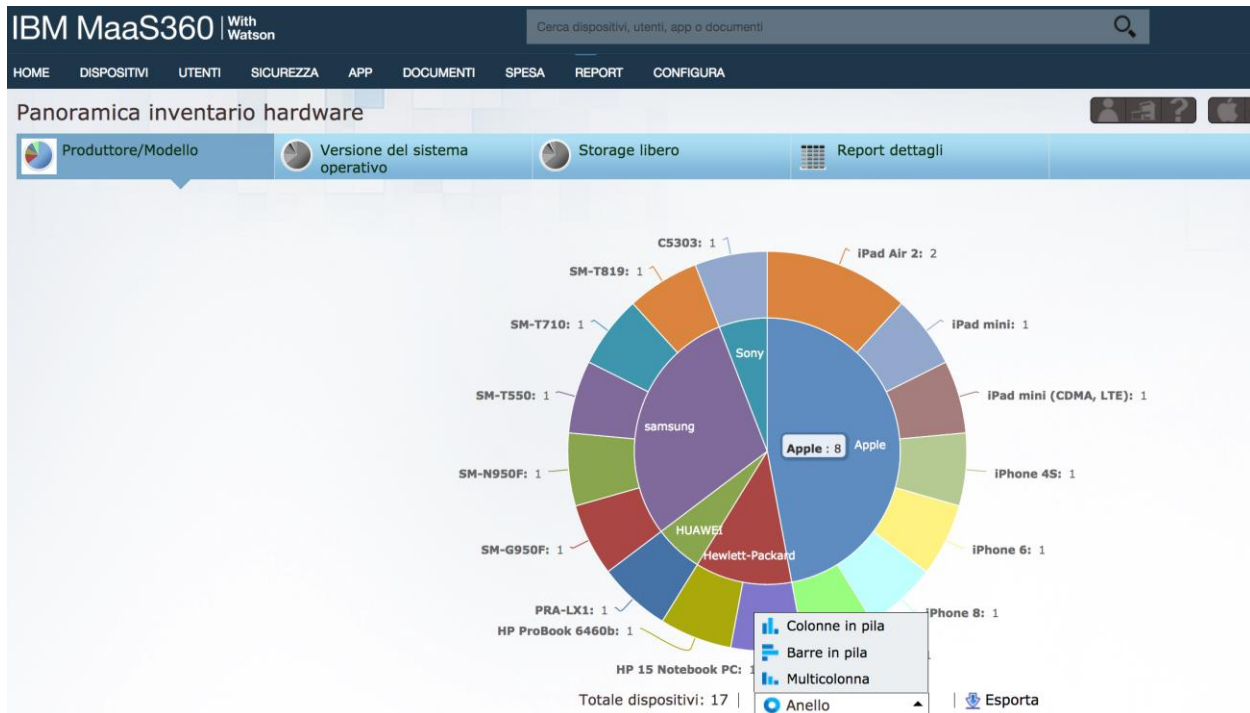
IBM MaaS360 With Watson			Cerca dispositivi, utenti, app o documenti		
HOME	DISPOSITIVI	UTENTI	SICUREZZA	APP	DOCUMENTI
Libreria contenuti: Tutti i documenti			Dispositivi mobili	Gestione delle spese mobili	Sicurezza del PC
			Panoramica MDM	Panoramica utilizzo dei dati	Sicurezza
			Inventario hardware	Analisi utilizzo dei dati	Antivirus
			Rete	Inventario PC	Firewall personale
			Panoramica SPS	Panoramica del PC	Codifica
			Informazioni su BlackBerry	Inventario hardware	Backup & Recovery
			Panoramica distribuzione	Rete	
			App mobili	Sistema operativo	
			Inventario app	Software	
			Sicurezza della mobilità	Disponibilità Windows 10	
			Panoramica sicurezza	Community Analytics	
			Violazioni del browser	Parametri mobili	
			Panoramica URL visitati		
			AUTI		NO

E' possibile tramite grafici avere le informazioni sull'ambiente MaaS.

Questa informazione è esportabile e interattiva (puoi cliccare su pezzi del grafico per ottenere più dettagli).



Questi report personalizzabili. Questo rende facile produrre dei report da consegnare a persone che non possono avere accesso al portale.



IBM MaaS360 | With Watson

Cerca dispositivi, utenti, app o documenti

HOME DISPOSITIVI UTENTI SICUREZZA APP DOCUMENTI SPESA REPORT CONFIGURA

Panoramica inventario hardware

Produttore/Modello Versione del sistema operativo Storage libero Report dettagli

Nome dispositivo	Nome utente	Piattaforma	Tipo di dispositivo	Produttore	Modello	Versione del sistema operativo	Storage totale (GB)	Storage libero (GB)	Stato gestito	Ultimo report
Dan's iPad Air 2	dpaquette	IOS	Tablet	Apple	iPad Air 2	11.4	56.57	25.96	Registrato	07/09/2018
Khaled's iPad	cidemo	IOS	Tablet	Apple	iPad Air 2	11.4	116.11	71.21	Registrato	07/09/2018

Ultimi 7 giorni