

# VMWARE WORKSPACE ONE

## Tabella di confronto delle versioni

Workspace ONE è una piattaforma di Digital Workspace basata sull'intelligence che consente di distribuire e gestire in modo semplice e sicuro qualsiasi app su qualunque dispositivo, integrando funzionalità di controllo dell'accesso, gestione delle applicazioni e gestione degli endpoint multipiattaforma. Le seguenti versioni sono disponibili come servizio cloud.

Grazie alle versioni di Workspace ONE è semplice per le organizzazioni ottenere in licenza il livello di tecnologia appropriato in base ai requisiti di utenti ed endpoint. La maggior parte delle organizzazioni sceglierà di acquistare in abbonamento un mix delle versioni Standard, Advanced ed Enterprise, che funzionano insieme per creare una singola piattaforma di Digital Workspace per tutta l'organizzazione.

		VERSIONE STANDARD	VERSIONE ADVANCED	VERSIONE ENTERPRISE	VERSIONE ENTERPRISE per VDI
<b>INTELLIGENCE E AUTOMAZIONE</b>					
<b>Report personalizzati</b>	È possibile progettare report personalizzati con dati relativi a dispositivi, applicazioni e utenti.	•	•	•	•
<b>Dashboard configurabili della cronologia</b>	Offrono informazioni dettagliate sull'utilizzo di dispositivi e app nel corso del tempo in modo da ottimizzare l'allocazione delle risorse e i rinnovi delle licenze.			•	•
<b>Funzionalità di analisi delle app e Aptelligent</b>	È possibile misurare il tasso di adozione delle app e il coinvolgimento in app nell'ambiente in uso, scoprendo così rapidamente le app più utilizzate e quantificando senza difficoltà il ROI dei deployment di app.			•	•
<b>Motore decisionale per l'automazione</b>	È possibile automatizzare i processi definendo delle regole che consentono di operare sulla base di un ampio gruppo di parametri.			•	•
<b>Workflow per la mobility</b>	Propone azioni e notifiche basate sul contesto, permettendo agli utenti di completare le attività nei sistemi aziendali back-end senza uscire da VMware Boxer.			•	•
<b>GESTIONE DELL'ACCESSO</b>					
<b>Portale di accesso</b>	Portale delle applicazioni per piattaforme mobili e desktop per l'installazione o l'avvio in varie applicazioni sul dispositivo endpoint. Comprende AirWatch App Catalog e Workspace ONE App Portal.	•	•	•	•
<b>Single Sign-on (SSO) federato</b>	Federazione Active Directory su app di terze parti o sviluppate internamente usando uno degli standard di federazione. Include la funzionalità Form-Fill per la password per SSO. <i>*Limitazioni delle funzionalità in base alla modalità di licenza per dispositivo.</i>	•*	•*	•*	•*

		VERSIONE STANDARD	VERSIONE ADVANCED	VERSIONE ENTERPRISE	VERSIONE ENTERPRISE per VDI
<b>GESTIONE DELL'ACCESSO</b>					
<b>SSO one-touch</b>	Possibilità di sfruttare la Mobile Application Management con autenticazione dei certificati e biometrica per un'autenticazione sicura delle applicazioni. <i>*Limitazioni delle funzionalità in base alla modalità di licenza per dispositivo.</i>	●*	●*	●*	●*
<b>Controllo dell'accesso condizionale</b>	Policy per il controllo dell'accesso alle applicazioni per limitare l'accesso alle applicazioni in base al livello di autenticazione dell'utente, alla piattaforma del dispositivo, all'intervallo di rete e all'applicazione. <i>*Limitazioni delle funzionalità in base alla modalità di licenza per dispositivo.</i>	●*	●*	●*	●*
<b>Provider di identità (IDP)</b>	Possibilità di fungere da database delle identità per gli account utente. <i>*Limitazioni delle funzionalità in base alla modalità di licenza per dispositivo.</i>	●*	●*	●*	●*
<b>Mobile Email Management</b>	Integrazione del controllo dell'accesso ActiveSync del server di posta tramite API server dirette PowerShell, Office 365 e Google Apps.	●	●	●	●
<b>Secure Email Gateway (SEG)</b>	Soluzione gateway in linea per fornire controllo dell'accesso al server di posta dell'ambiente di lavoro e crittografare dati e allegati.		●	●	●
<b>VMware PIV-D Manager</b>	Possibilità di applicare l'autenticazione a due fattori attraverso un certificato client per credenziali derivate utilizzando VMware PIV-D Manager.		●	●	●
<b>PROTEZIONE DI APP E DATI</b>					
<b>VMware Browser</b>	Applicazione di navigazione Intranet per proteggere l'accesso alle applicazioni web.		●	●	●
<b>VMware Content Locker</b>	Aggregazione e visualizzazione dei file su repository di file on-site e basati su cloud. Comprende Mobile Content Management, oltre a modifica e annotazione di file, proteggendo al contempo dalla perdita di dati con limitazioni per le operazioni "apri in" e taglia/copia/incolla. Combina funzionalità Content Locker standard e avanzate.		●	●	●
<b>VMware Boxer</b>	Offre ai dipendenti un servizio e-mail sicuro, migliore di quello nativo, con incredibili funzionalità dedicate alla produttività per posta, calendario e contatti.		●	●	●
<b>VMware People Search</b>	I dipendenti possono cercare rapidamente i colleghi, accedere a informazioni di contatto complete, visualizzare organigrammi ed effettuare chiamate o inviare e-mail attraverso l'applicazione VMware People Search.		●	●	●
<b>Mobile Application Management</b>	Possibilità di installare, configurare e assegnare le applicazioni (interne, pubbliche, web, native ecc.) a utenti e dispositivi, nonché di monitorarne l'inventario.	●	●	●	●

		VERSIONE STANDARD	VERSIONE ADVANCED	VERSIONE ENTERPRISE	VERSIONE ENTERPRISE per VDI
<b>PROTEZIONE DI APP E DATI</b>					
<b>Container e SDK con DLP Protection</b>	Contenimento app tramite MAM e AirWatch Software Development Kit (SDK) indipendenti.	●	●	●	●
<b>Wrapping delle app</b>	Possibilità di aggiungere policy di sicurezza e funzionalità di gestione a un'app già sviluppata.		●	●	●
<b>VMware Tunnel</b>	Soluzione VPN per app per la connessione delle applicazioni (di VMware o di terze parti) a servizi della Intranet aziendale. Include l'integrazione di VMware Tunnel e VMware NSX.		●	●	●
<b>GESTIONE UNIFICATA DEGLI ENDPOINT</b>					
<b>Mobile Device Management (MDM)</b>	Possibilità di configurare policy dei dispositivi, impostazioni e configurazioni dei dispositivi su telefoni, tablet e laptop.	●	●	●	●
<b>Gestione di dispositivi specifici (OEM)</b>	Tecnologia speciale per la gestione di dispositivi condivisi, chiosco e rinforzati. Comprende API aggiuntive per la gestione di dispositivi specifici OEM e supporto per piattaforme legacy, tra cui Android OEM, Samsung Knox, Windows CE, Windows Mobile, QNX, ecc.	●	●	●	●
<b>Gestione di periferiche e dispositivi indossabili</b>	Possibilità di gestire dispositivi indossabili e periferiche come smart glass, stampanti o altri accessori.	●	●	●	●
<b>Assistenza e diagnostica over-the-air</b>	Strumenti di risoluzione dei problemi, diagnostica e assistenza remoti per eseguire e terminare i processi (oltre che acquisire i registri) a distanza.	●	●	●	●
<b>Gestione desktop avanzata</b>	Comprende script personalizzati, crittografia BitLocker, gestione di app desktop/Win32, policy di Windows 10 (tra cui Credential Guard, Device Guard).		●	●	●
<b>Strumenti di gestione delle telecomunicazioni</b>	Funzionalità di gestione delle telecomunicazioni per monitorare i dati e l'utilizzo di chiamate e messaggi, oltre che per automatizzare azioni e compliance.		●	●	●
<b>Motore per l'automazione della compliance IT</b>	Possibilità di creare policy di compliance con workflow di correzione automatizzati, quali ad esempio whitelist/blacklist delle applicazioni, GPS e geofencing, controllo della versione del sistema operativo ed escalation della compliance.	●	●	●	●
<b>AirLift per Windows 10</b>	Connettore lato server di gestione congiunta per Microsoft System Center Configuration Manager (SCCM), che rende meno rischiosa e accelera la transizione delle attività di gestione dei PC tradizionalmente complesse alla gestione moderna di Workspace ONE per Windows 10.	●	●	●	●

		VERSIONE STANDARD	VERSIONE ADVANCED	VERSIONE ENTERPRISE	VERSIONE ENTERPRISE per VDI
<b>APP E DESKTOP VIRTUALI</b>					
<b>App virtuali (Horizon)</b>	Possibilità di distribuire applicazioni virtuali sui dispositivi.			●	●
<b>Desktop virtuali (Horizon)</b>	Possibilità di distribuire applicazioni e/o desktop virtuali sui dispositivi.				●
<b>Numero di dispositivi con licenza</b>					
	Numero massimo di dispositivi consentiti nella gestione o app SDK gestita.	Licenza per dispositivo: 1 Licenza per utente: 5	Licenza per dispositivo: 1 Licenza per utente: 5	Licenza per dispositivo: 1 Licenza per utente: 5	Licenza per dispositivo: 1 Licenza per utente: 5
<b>Accesso al portale Workspace ONE</b>					
	Numero massimo di dispositivi che possono accedere al portale Workspace ONE tramite un browser senza essere gestiti.	Licenza per dispositivo: 1 Licenza per utente: illimitata	Licenza per dispositivo: 1 Licenza per utente: illimitata	Licenza per dispositivo: 1 Licenza per utente: illimitata	Licenza per dispositivo: 1 Licenza per utente: illimitata

\* Se Workspace ONE viene concesso in licenza per singolo dispositivo, la tecnologia di SSO e controllo dell'accesso funziona esclusivamente sui dispositivi gestiti e a partire dalle applicazioni gestite. Per abilitare l'accesso alle applicazioni aziendali dai dispositivi non gestiti da AirWatch oppure consentirne l'accesso da qualsiasi browser web, è necessario optare per il modello di licenza per singolo utente di Workspace ONE.

Per ulteriori informazioni su Workspace ONE, visitare il sito: [vmware.com/go/workspaceone](http://vmware.com/go/workspaceone).

