

# JUNIPER MIST ACCESS ASSURANCE

## Panoramica del prodotto

[Juniper Mist Access Assurance](#) è un servizio basato su cloud che garantisce l'accesso di rete zero trust e basato sull'identità, oltre a assegnazioni complete di policy e segmentazione dello stack con visibilità dell'esperienza utente end-to-end. Il servizio offre una suite di funzionalità di controllo degli accessi con un framework di policy di autorizzazione flessibile ma semplice per l'onboarding di guest, IoT, BYOD e dispositivi aziendali. La connessione client è controllata in base alle identità degli utenti e dei dispositivi, regolando l'accesso per i dispositivi che si connettono alla rete. Access Assurance fornisce anche servizi di controllo degli accessi per i dispositivi che sfruttano l'autenticazione 802.1X e il bypass degli indirizzi MAC per i dispositivi IoT cablati non autorizzati 802.1X.

## Descrizione prodotto

Juniper® Mist™ Access Assurance è un servizio di controllo degli accessi di rete (NAC) cloud basato su microservizi che consente alle aziende di applicare facilmente un modello di sicurezza zero trust. Access Assurance risolve molte problematiche di complessità associate alle offerte NAC tradizionali:

- Rimozione dell'hardware del server on-premise
- Fornire servizi intrinsecamente altamente disponibili e resilienti
- Abilitazione di aggiornamenti automatici delle funzionalità in tempo di esecuzione, sicurezza, e correzioni delle vulnerabilità

Access Assurance va oltre le funzionalità di [Juniper Mist IoT Assurance](#), che semplifica l'onboarding per i dispositivi IoT e BYOD headless. Con Access Assurance, i team IT possono integrare dispositivi cablati e wireless con metodi di autenticazione 802.1X o MAC Authentication Bypass (MAB), anche per dispositivi non 802.1X.

Access Assurance utilizza centinaia di vettori diversi per abbinare l'identità dell'utente e del dispositivo, come gli attributi dei certificati X.509, le iscrizioni ai gruppi di utenti, le metriche di compliance e postura dei dispositivi e il contesto della posizione. Questi vettori contribuiscono a determinare i criteri di ammissione di rete basati sull'identità, come il segmento di rete o il microsegmento a cui un dispositivo dovrebbe connettersi e la policy di rete che dovrebbe essere applicata dinamicamente a un utente.

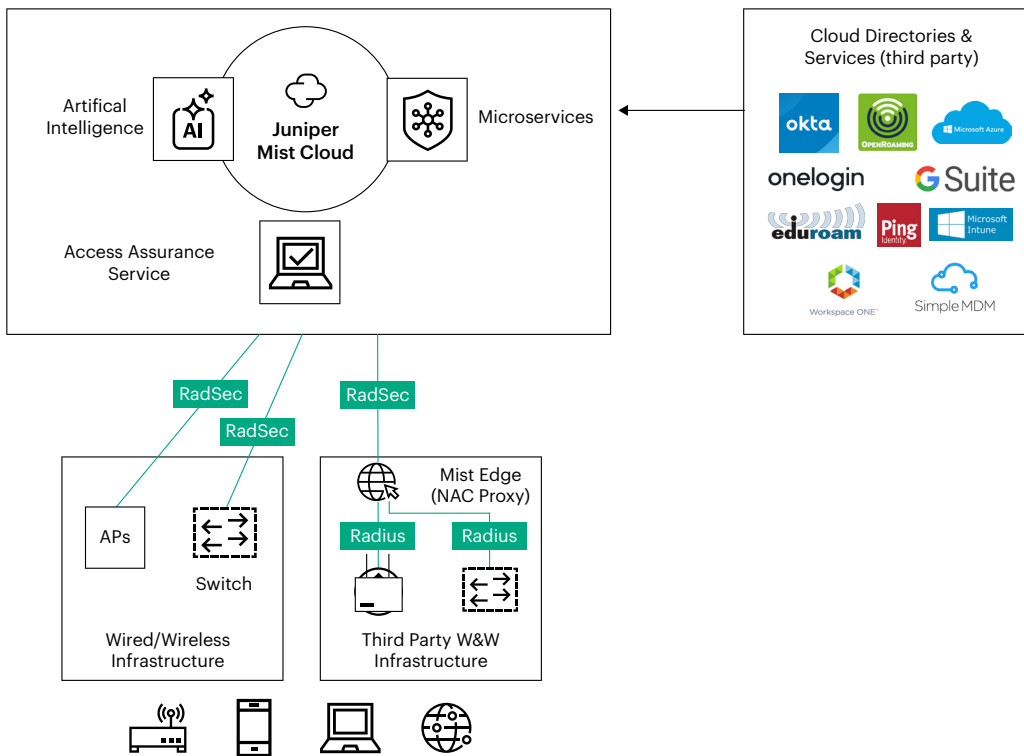


Figura 1. Il servizio cloud Juniper Mist Access Assurance semplifica notevolmente il controllo degli accessi di rete

Org Policies

Each user/resources session is evaluated according to the list of Policy rules. The policy for the first matching rule is applied.

| No.  | Name                    | Match Criteria (match on location, SSID, User Group, etc)                             | Policy                 | Assigned Policies (VLAN, Roles, Session Timeouts, etc) |
|------|-------------------------|---|------------------------|--|
| 1    | Deny Banned Devices     | Banned Device   | Network Access Denied  |  |
| 2    | Approved Wired Printers | + all ApprovedPrinters MAB Wired  | Network Access Allowed | Printers IoTNetwork                                    |
| 3    | Approved Wired Cameras  | + all ApprovedCameras MAB Wired   | Network Access Allowed | Cameras IoTNetwork                                     |
| 4    | Mist Access Points      | + all Mist Access Points MAB Wired  | Network Access Allowed | Mist AP Role Network Infrastructure Group              |
| 5    | Wired Cert Auth         | + any Employee Group Contractors Group<br>all Cert issued by Juniper EAP-TLS Wired    | Network Access Allowed | Employee Network Trusted-Device-Group                  |
| 6    | Employee BYOD           | + any Employee Group Contractors Group<br>all EAP-TLS Wireless                        | Network Access Allowed | Employee Role BYOD Network                             |
| 7    | Employee CORP Devices   | + any Employee Group Contractors Group<br>all Cert issued by Juniper EAP-TLS Wireless | Network Access Allowed | Employee Network Employee Role                         |
| Last |                         | All Users   | Network Access Denied  |  |

Figura 2. L'interfaccia flessibile per la creazione di policy aiuta gli amministratori ad assegnare le policy in base ai requisiti aziendali

Ancora più importante, Access Assurance fornisce la risoluzione dei problemi di connettività end-to-end in una vista unificata dal punto di vista del client, dell'infrastruttura di rete e del controllo degli accessi, semplificando notevolmente il supporto del Giorno 2. Gli amministratori IT ottengono una visione coerente dell'esperienza dell'utente finale e possono determinare se le esperienze negative sono dovute alla configurazione del client, all'infrastruttura di rete, all'autenticazione o a un servizio.

Client Events 127 Total 119 Good 2 Neutral 6 Bad

|   |               |                         |                           |                               |                    |   |
|---|---------------|-------------------------|---------------------------|-------------------------------|--------------------|---|
| Gateway ARP Success                       | APHX-BRQLAB-1 | 12:59:18.965 PM, Feb 16 | SSID                      | mist-aa                       | VLAN               | 750   |
| DHCP Success                              | APHX-BRQLAB-1 | 12:59:18.964 PM, Feb 16 | Certificate Serial Number | 8bbc1f01739ab6e9              | User Group         | employee  |
| Authorization & Association               | APHX-BRQLAB-1 | 12:59:18.378 PM, Feb 16 | Authentication Type       | 802.1X                        | User Name          | user1@deaflyz.onmicrosoft.com                   |
| NAC Authorization Success                 | APHX-BRQLAB-1 | 12:59:18.298 PM, Feb 16 | Certificate CN            | user1@deaflyz.onmicrosoft.com | Certificate Issuer | /C=US/ST=CA/O=Mist/CN=ca.deaflyzonmicrosoft.com |
| NAC IDP Group Lookup Success              | APHX-BRQLAB-1 | 12:59:18.296 PM, Feb 16 | Certificate Expiry        | 2033-02-06T09:55:32Z          | EAP Type           | EAP-TLS   |
| NAC Client Certificate Validation Success | APHX-BRQLAB-1 | 12:59:18.282 PM, Feb 16 |                           |                               | IdP Roles          | UNCG-Portal-UsersEmployee                       |
|   |               |                         |                           |                               | Auth Rule          | Employee CORP Devices                           |

Figura 3. Il client SLE monitora gli eventi di controllo degli accessi di rete

# Architettura e componenti chiave

Access Assurance viene fornita tramite il [cloud Juniper-Mist](#) e basata su [Mist AI](#). L'architettura dei microservizi unisce disponibilità elevata, ridondanza e scalabilità automatica per un accesso di rete ottimale su reti [cablate](#), [Wi-Fi](#) e [WAN](#). Utilizzando la geoawareness, Access Assurance reindirizza automaticamente le richieste di autenticazione da diverse regioni all'istanza Access Assurance più vicina per fornire latenza minima e la migliore esperienza per l'utente finale.

Access Assurance fornisce un servizio di autenticazione integrando servizi di directory esterni, come Google Workspace™, Microsoft Azure AD, Okta Identity e altri. Integra inoltre fornitori esterni di infrastrutture a chiave pubblica (PKI) e gestione dei dispositivi mobili (MDM), come Jamf, Microsoft Intune e altri, per fornire un'identificazione granulare di utenti e dispositivi per applicare il controllo degli accessi alla rete zero trust basato sull'identità.

## Caratteristiche e vantaggi

### Dare priorità alle esperienze dei clienti

Access Assurance fornisce una vista unificata dell'esperienza di connettività client e può identificare facilmente un problema ed eseguire l'analisi delle cause radice. Tutti gli eventi client, inclusi i successi e i fallimenti di connessione e autenticazione, vengono acquisiti dal cloud Juniper Mist. Con questo dati, il cloud Juniper Mist contribuisce a semplificare le operazioni quotidiane identificando facilmente se un problema di connettività dell'utente finale è causato da un errore di configurazione del client, problemi di infrastruttura e servizio di rete o problemi di configurazione delle policy di autenticazione. Le aspettative sul livello di servizio (SLE) di Juniper Mist per i client [cablati](#) e [wireless](#) sono migliorate per includere eventi di accesso alla rete, come eventi di autenticazione, convalide dei certificati e altro ancora.

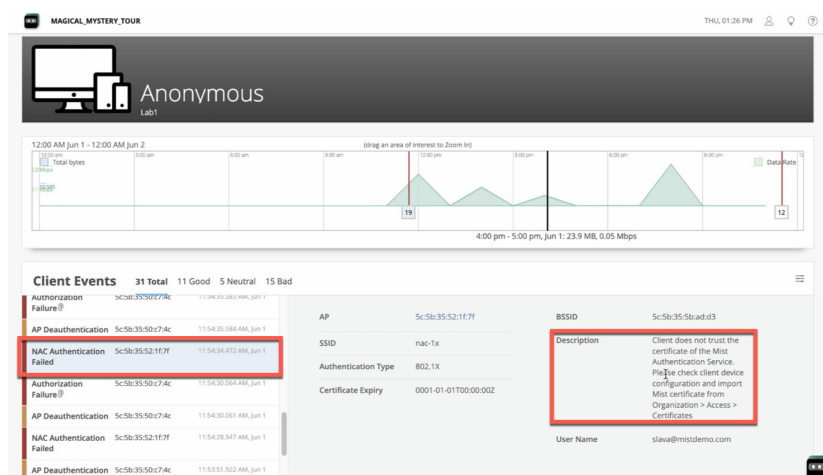


Figura 4. I guasti del LES client forniscono descrizioni per problemi noti

## Un unico pannello di controllo per la gestione e le operazioni

Access Assurance è strettamente integrato con il cloud Juniper Mist, fornendo gestione full-stack e operazioni quotidiane per [Wi-Fi Assurance](#), [Wired Assurance](#), [SD-WAN Assurance](#) e Access Assurance in un unico dashboard per una visibilità end-to-end. Il motore [Marvis® AI Assistant](#) sfrutta i dati provenienti da più origini per il rilevamento delle anomalie per fornire metriche fruibili. Attraverso il dashboard, gli utenti possono:

- Creare e applicare policy di accesso che garantiscano solo l'autorizzazione ai dispositivi e agli utenti è consentito l'accesso alla rete
- Assegnare utenti e dispositivi al segmento di rete corretto
- Impedire a utenti e dispositivi di accedere a risorse limitate
- Aggiungere e modificare certificati e autorità di certificazione
- Configurazione dei provider di identità
- Monitorare l'attività dei clienti in tutta l'organizzazione

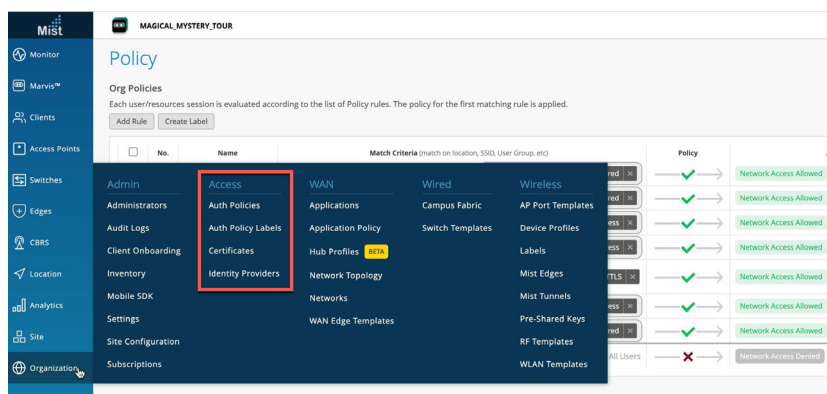


Figura 5. Un'interfaccia utente intuitiva evidenzia i controlli di accesso

## Identità granulare di utenti e dispositivi

Access Assurance è in grado di eseguire il fingerprinting granulare delle identità in base agli attributi del certificato X.509. Utilizza anche informazioni sul provider di identità (IdP) come l'appartenenza al gruppo, lo stato dell'account utente, lo stato di compliance MDM, gli elenchi dei client e la posizione dell'utente per l'impronta digitale. L'impronta digitale dell'utente e del dispositivo risultante fornisce un vettore di identità per un'assegnazione accurata delle policy all'interno dei principi zero trust.

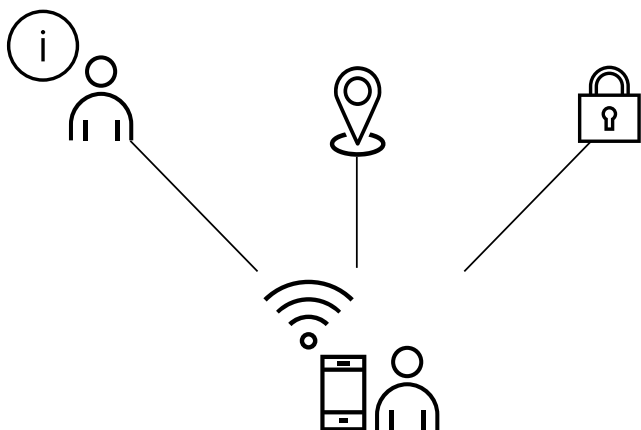


Figura 6. L'impronta digitale dell'identità è possibile attraverso più metodi

## Applicazione delle policy di rete e microsegmentazione

In base all'identità dell'utente e del dispositivo, Access Assurance può richiedere alla rete di assegnare un utente a un segmento di rete specifico (VLAN o un tag di policy basato su gruppo), oltre a applicare la policy di rete assegnando un ruolo utente. Tali ruoli possono essere sfruttati nel framework delle policy WxLAN di Juniper Mist o nelle policy di switch.



Figura 7. Le policy applicate per VLAN, policy basate su gruppi e ruoli utente sono facilmente visibili

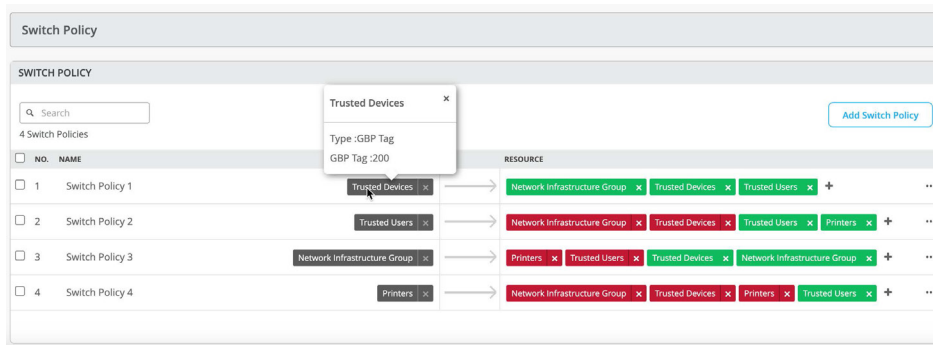


Figura 8. Riconoscere le policy con tag basati su gruppi è rapido e veloce

## Elevata disponibilità e geo-affinità integrate

Con Access Assurance, le organizzazioni ottengono affidabilità e bassa latenza controllo degli accessi di rete delle loro reti in distribuzioni singole e multisito. HPE ha distribuito istanze cloud del suo servizio cloud di controllo degli accessi di rete in più sedi regionali. Nelle distribuzioni multisito, il traffico di autenticazione proveniente dall'infrastruttura di rete viene automaticamente indirizzato all'istanza Access Assurance più vicina. La latenza è ridotta al minimo e gli utenti godono di un'esperienza wireless eccezionale. Questo processo automatizzato è completamente trasparente per gli utenti e non richiede alcun coinvolgimento da parte del team IT. Alle organizzazioni è garantito un accesso di rete affidabile e ridondante per i dispositivi client, indipendentemente dallo stato dell'istanza regionale più vicina.

## Aggiornamenti automatici delle funzionalità e della sicurezza

L'architettura cloud basata su microsistemi di Juniper Mist mantiene Access Assurance ottimizzato con le tecnologie più avanzate. Nuove funzionalità, patch di sicurezza e aggiornamenti vengono aggiunti automaticamente a Access Assurance su base bisettimanale senza interruzioni o downtime dei servizi. Questa funzionalità semplifica e migliora notevolmente le operazioni di servizio per gli amministratori IT di rete, eliminando lunghi upgrade software e downtime dei servizi. HPE è in grado di distribuire con facilità nuove funzionalità e funzionalità ai suoi servizi basati su cloud, portando i progressi sul mercato in modo più rapido e migliorando continuamente la tua esperienza client-to-cloud.

## Access Assurance estende Juniper Mist IoT Assurance

Access Assurance è abbinato a Juniper Mist IoT Assurance per creare controlli per l'onboarding e la gestione dei dispositivi aziendali con autenticazione 802.1X e onboarding senza MAC di dispositivi IoT e BYOD non 802.1X. Le funzionalità di IoT Assurance semplificano le operazioni IT e le connessioni sicure per i dispositivi IoT e BYOD headless tramite un meccanismo MPSK (Multiple Pre-Shared Key). Incorpora una suite completa di funzionalità di controllo degli accessi che sfrutta MPSK o Private Pre-Shared Key (PPSK) come nuovo tipo di identità e vettore di policy.

IoT Assurance fornisce anche la creazione del portale PSK, consentendo i flussi di lavoro di onboarding BYOD automatizzando la generazione di PSK in base all'identità dell'utente, sfruttando il linguaggio di marcatura delle asserzioni di sicurezza (SAML) per un'esperienza SSO. Consente l'onboarding senza problemi dei dispositivi client tramite codice QR mobile o digitando una passphrase personalizzata senza installare alcun software client.

Gli abbonamenti a Access Assurance includono la funzionalità IoT Assurance per un semplice controllo degli accessi per tutti i client e i dispositivi della rete, indipendentemente dal modo in cui si connettono.

## Assistente di rete virtuale Marvis

[Marvis Virtual Network Assistant](#) utilizza Mist AI per aiutare i team IT a interagire e interagire con le loro reti. Il motore Marvis AI unisce Access Assurance ad altri Juniper Mist servizi basati su cloud, come Wired Assurance, Wi-Fi Assurance e WAN Assurance, che aiutano il team operativo ad avvicinarsi al raggiungimento di The Self-Driving Network™ con risoluzione dei problemi e analisi delle prestazioni semplificate.

Utilizzando le funzionalità basate su Mist AI, il personale dell'help desk e gli amministratori di rete possono semplicemente porre una domanda in linguaggio naturale e ottenere informazioni fruibili utilizzando l'interfaccia conversazionale Marvis che li aiuta a identificare e risolvere i problemi di rete. Marvis porta il rilevamento proattivo delle anomalie nel dashboard SLE. Con Marvis Actions, il personale ottiene informazioni proattive e fruibili per identificare i problemi di accesso alla rete nell'intero stack, fornendo suggerimenti per i problemi di connettività degli utenti. In questo modo, i nostri clienti possono eseguire facilmente l'analisi delle cause radice nell'intero stack di rete e nei servizi di autenticazione.

## Architettura basata su API

Il servizio Access Assurance si basa al 100% su API REST (Representational State Transfer) pubbliche che consentono una facile integrazione con i sistemi SIEM (SIEM) o di gestione dei servizi IT o altre piattaforme per l'assegnazione di configurazione e policy. Queste API forniscono la capacità di invocare azioni basate su eventi utente o esterni, nonché di utilizzare il framework Webhook cloud-native. Nel complesso, la piattaforma Juniper Mist è programmabile al 100%, utilizzando OpenAPI, per la piena automazione e integrazione senza interruzioni con accesso HPE Juniper Networking complementare, cablato, wireless, WAN, sicurezza, soluzioni di [coinvolgimento degli utenti](#) e [visibilità degli asset](#).

# Specifiche

| Funzionalità   | Description  |
|--|--|
| Gestione dei certificati X.509   | Supporto PKI esterno<br>Controllo automatico della revoca dei certificati CRL/OSCP   |
| Integrazione con il provider di identità esterno                                   | I seguenti protocolli sono supportati per l'integrazione in qualsiasi provider di identità per eseguire la ricerca degli utenti e ottenere informazioni sullo stato del dispositivo: <ul style="list-style-type: none"><li>— Secure Lightweight Directory Access Protocol (LDAP)</li><li>— OAuth2</li><li>— accesso di rete sicuro eduroam</li><li>— Integrazioni continuamente aggiunte per i principali tool di gestione unificata degli endpoint (UEM), gestione della mobilità aziendale (EMM) e gestione dei dispositivi mobili (MDM)</li></ul> |
| Metodi di autenticazione 802.1X  | I seguenti metodi EAP sono supportati per l'accesso 802.1X protetto: <ul style="list-style-type: none"><li>— Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)</li><li>— Tunnel PEAP TLS per protocollo di autenticazione estensibile protetto</li><li>— Extensible Authentication Protocol (TEAP) (TLS/TLS)</li><li>— Protocollo di autenticazione estensibile - TLS tunnelizzato (EAPTTLS (PAP))</li></ul>   |
| Metodi di autenticazione Non-802.1X  | Bypass di autenticazione MAC (MAB)<br>Multi-Pre-Shared Key (MPSK)  |
| Policy di rete e microsegmentazione  | Assegnazione dinamica di VLAN, ruoli e tag di policy basati su gruppi in base a l'identità dell'utente   |
| Rete di terzi supporto dell'infrastruttura   | Supportato tramite l'applicazione Mist Edge Auth Proxy, dispositivi di fornitori terzi può comunicare tramite RADIUS standard al proxy Mist Edge Auth  |
| Garanzia IoT di Juniper Mist (Incluso con tutti gli accessi Abbonamenti Assurance) | Onboarding dei dispositivi client IoT e BYOD <ul style="list-style-type: none"><li>— Crea, ruota, escludi automaticamente PSK e MPSK</li><li>— Ingegneria dinamica del traffico</li><li>— Policy WxLAN basata su chiavi</li><li>— Creazione e gestione della WLAN personale</li><li>— Monitoraggio attivo dell'utilizzo dei dispositivi in base a PSK</li><li>— Provisioning e rotazione automatizzati delle chiavi</li></ul>  |

## Informazioni per l'ordinazione

Il servizio Access Assurance viene fornito in abbonamento, in base alla media dei dispositivi client attivi contemporaneamente osservati nell'arco di un periodo di 7 giorni.

Gli abbonamenti standard includono tutte le funzionalità di controllo degli accessi di rete all'interno del cloud Juniper Mist.

Le sottoscrizioni avanzate aggiungono il controllo della postura del client (UEM/EMM/ MDM) e le integrazioni del firewall alle funzionalità standard di Access Assurance.

| SKU          | Description   |
|--------------|---|
| S-CLIENT-S-1 | Abbonamento Standard Access & IoT Assurance per 1 client per 1 anno |
| S-CLIENT-S-3 | Abbonamento Standard Access & IoT Assurance per 1 client per 3 anni |
| S-CLIENT-S-5 | Abbonamento Standard Access & IoT Assurance per 1 client per 5 anni |
| S-CLIENT-A-1 | Abbonamento Advanced Access e IoT Assurance per 1 client per 1 anno |
| S-CLIENT-A-3 | Abbonamento Advanced Access & IoT Assurance per 1 client per 3 anni |
| S-CLIENT-A-5 | Abbonamento Advanced Access & IoT Assurance per 1 client per 5 anni |

## Informazioni su HPE

HPE è leader nella tecnologia aziendale essenziale, che riunisce la potenza dell'AI, del cloud e del networking per aiutare le organizzazioni a ottenere di più. In qualità di pionieri delle possibilità, la nostra innovazione e le nostre competenze promuovono il modo in cui le persone vivono e lavorano. Supportiamo i nostri clienti in tutti i settori per ottimizzare le prestazioni operative, trasformare i dati in previsioni e massimizzarne l'impatto. Libera le tue ambizioni più audaci con HPE. Scopri di più su [HPE.com](https://www.hpe.com).

**Esclusione di responsabilità:** La presente scheda tecnica è stata tradotta in tedesco/francese/italiano/spagnolo/giapponese/coreano utilizzando l'intelligenza artificiale per maggiore praticità. Si noti che la traduzione non è stata rivista o verificata da traduttori umani e, come risultato, ci potrebbero essere errori o alterazioni linguistiche di piccola entità. Per informazioni più precise e affidabili, consultare la versione originale della scheda tecnica in lingua inglese.

[Visita HPE.com](https://www.hpe.com)

### [Avvia chat](#)

© Copyright 2025 Hewlett Packard Enterprise Development LP. Le informazioni contenute nel presente documento sono soggette a modifica senza preavviso. Le uniche garanzie per i prodotti e i servizi Hewlett Packard Enterprise sono quelle espressamente indicate nelle dichiarazioni di garanzia esplicite che accompagnano tali prodotti e servizi. Nulla di quanto contenuto nel presente documento potrà essere interpretato come garanzia supplementare. Hewlett Packard Enterprise non sarà responsabile per errori tecnici o editoriali o omissioni qui contenute.

Google Workspace è un marchio registrato di Google LLC. Azure, Microsoft e Microsoft Intune sono marchi o marchi registrati di Microsoft Corporation negli Stati Uniti e/o in altri Paesi. Tutti i marchi di terzi appartengono ai rispettivi titolari.

a00150852ite

HEWLETT PACKARD ENTERPRISE

[hpe.com](https://www.hpe.com)

