

# Dell Wyse Management Suite

Guida introduttiva rapida versione 3.x



## Messaggi di N.B., Attenzione e Avvertenza

 **N.B.:** un messaggio N.B. (Nota Bene) indica informazioni importanti che contribuiscono a migliorare l'utilizzo del prodotto.

 **ATTENZIONE:** un messaggio di **ATTENZIONE** evidenzia la possibilità che si verifichi un danno all'hardware o una perdita di dati ed indica come evitare il problema.

 **AVVERTENZA:** un messaggio di **AVVERTENZA** evidenzia un potenziale rischio di danni alla proprietà, lesioni personali o morte.

|   |           |
|---|-----------|
| <b>Capitolo 1: Introduzione</b>   | <b>5</b>  |
| Matrice di funzioni di Wyse Management Suite  | 5         |
| <b>Capitolo 2: Guida introduttiva a Wyse Management Suite</b>   | <b>11</b> |
| Accesso a Wyse Management Suite su public cloud   | 11        |
| Prerequisiti per l'implementazione di Wyse Management Suite su private cloud                                | 12        |
| <b>Capitolo 3: Installazione di Wyse Management Suite sul private cloud</b>                                 | <b>13</b> |
| Accesso a Wyse Management Suite   | 21        |
| Aree funzionali della console di gestione   | 21        |
| Configurazione e gestione dei thin client   | 21        |
| Creazione del gruppo di criteri e aggiornamento della configurazione  | 23        |
| Registrazione del nuovo thin client   | 23        |
| Registrazione manuale del dispositivo ThinOS  | 24        |
| Registrazione dei dispositivi mediante i tag di opzione DHCP  | 25        |
| Registrazione dei dispositivi mediante il record DNS SRV  | 26        |
| Registrazione dei dispositivi mediante i campi del record DNS protetto o le opzioni di ambito DHCP protetto | 28        |
| <b>Capitolo 4: Distribuzione di applicazioni ai thin client</b>   | <b>29</b> |
| Caricamento e distribuzione dell'inventario di immagini firmware ThinOS                                     | 29        |
| Creazione e distribuzione del criterio di applicazione standard ai thin client                              | 29        |
| <b>Capitolo 5: Aggiornamento di Wyse Management Suite dalla versione 2.x alla 3.x</b>                       | <b>31</b> |
| <b>Capitolo 6: Aggiornamento di Wyse Management Suite dalla versione 3.x alla 3.3</b>                       | <b>32</b> |
| <b>Capitolo 7: Aggiornamento di Wyse Management Suite dalla versione 3.x alla 3.5</b>                       | <b>33</b> |
| <b>Capitolo 8: Aggiornamento di Wyse Management Suite dalla versione 3.x alla 3.6</b>                       | <b>35</b> |
| <b>Capitolo 9: Disinstallazione di Dell Wyse Management Suite</b>   | <b>37</b> |
| <b>Capitolo 10: Risoluzione dei problemi di Dell Wyse Management Suite</b>                                  | <b>38</b> |
| <b>Capitolo 11: Wyse Device Agent</b>   | <b>40</b> |
| <b>Capitolo 12: Risorse aggiuntive</b>  | <b>41</b> |
| <b>Appendice A: Database remoto</b>   | <b>42</b> |
| Configurazione del database Mongo   | 42        |
| Configurazione del database Maria   | 43        |

|   |           |
|---|-----------|
| <b>Appendice B: Installazione personalizzata.....</b>   | <b>45</b> |
| <b>Appendice C: Accedere al repository di file di Wyse Management Suite.....</b>                        | <b>50</b> |
| <b>Appendice D: Creazione e configurazione dei tag di opzione DHCP.....</b>                             | <b>53</b> |
| <b>Appendice E: Creazione e configurazione dei record DNS SRV.....</b>                                  | <b>59</b> |
| <b>Appendice F: Creazione e distribuzione del criterio di applicazione standard ai thin client.....</b> | <b>66</b> |
| <b>Appendice G: Registrazione manuale di Dell Hybrid Client.....</b>                                    | <b>67</b> |
| <b>Appendice H: Registrazione manuale dei dispositivi Windows Embedded Standard.....</b>                | <b>69</b> |
| <b>Appendice I: Registrazione manuale del dispositivo ThinOS 8.x.....</b>                               | <b>70</b> |
| <b>Appendice J: Registrazione manuale del dispositivo ThinOS 9.x.....</b>                               | <b>71</b> |
| <b>Appendice K: Registrazione manuale dei dispositivi Linux.....</b>                                    | <b>72</b> |
| <b>Appendice L: Termini e definizioni.....</b>  | <b>73</b> |

# Introduzione

Wyse Management Suite è la soluzione di gestione e di nuova generazione che consente di configurare, monitorare, gestire e ottimizzare centralmente gli endpoint basati su Dell Hybrid Client e i thin client Dell. Inoltre, offre opzioni di funzionalità avanzate come l'implementazione su cloud e on-premise, l'opzione di gestione da qualsiasi posizione utilizzando un'applicazione mobile, la sicurezza avanzata, ad esempio la configurazione del BIOS, e il blocco delle porte. Altre funzioni includono rilevamento e registrazione dei dispositivi, gestione di asset e inventario, gestione della configurazione, implementazione di sistemi operativi e applicazioni, comandi in tempo reale, monitoraggio, avvisi, creazione di report e risoluzione dei problemi degli endpoint.

## Edizioni

Wyse Management Suite è disponibile nelle seguenti edizioni:

- **Standard (gratuita):** la Standard Edition di Wyse Management Suite offre funzionalità di base ed è disponibile solo per l'implementazione su private cloud. Non è richiesto un codice di licenza per usare la Standard Edition. Questa versione è in grado di gestire i thin client Dell. La Standard Edition è adatta per piccole e medie imprese.
- **Pro (a pagamento):** la Pro Edition di Wyse Management Suite è una soluzione più strutturata. È disponibile per l'implementazione su public e private cloud. Per utilizzare la Pro Edition (licenze basate su abbonamento) è necessario un codice di licenza. La soluzione Pro consente alle organizzazioni di adottare un modello ibrido e di alternare licenze private e public cloud, se necessario. Questa versione è necessaria per gestire qualsiasi dispositivo basato su Teradici, Wyse Covert per PC e i dispositivi basati su Dell Hybrid Client. Offre inoltre funzionalità più avanzate per la gestione dei thin client Dell. Per l'implementazione su public cloud, la Pro Edition può essere gestita su reti non aziendali (home office, terze parti, partner, thin client mobili e così via). La Pro Edition di Wyse Management Suite offre inoltre:
  - Un'applicazione mobile per visualizzare gli avvisi e le notifiche critici e inviare i comandi in tempo reale.
  - Protezione avanzata attraverso l'autenticazione a due fattori e l'autenticazione Active Directory per l'amministrazione basata sui ruoli.
  - Policy app avanzate e reporting.

### **i** N.B.:

- I servizi cloud sono in hosting negli Stati Uniti e in Germania. I clienti nei Paesi con restrizioni sulla posizione dei dati potrebbero non essere in grado di sfruttare il vantaggio del servizio basato su cloud di Wyse Management Suite Pro.
- La versione on-premise di Wyse Management Pro Edition è la soluzione migliore per i clienti con restrizioni in termini di residenza dei dati.

### Argomenti:

- [Matrice di funzioni di Wyse Management Suite](#)

## Matrice di funzioni di Wyse Management Suite

La tabella seguente fornisce informazioni sulle funzioni che sono supportate per ciascun tipo di abbonamento.

**Tabella 1. Matrice della funzione per ciascun tipo di abbonamento**

| Funzioni  | Wyse Management Suite Standard     | Wyse Management Suite Pro - Private cloud | Wyse Management Suite Edition Pro - Cloud Edition |
|---|------------------------------------|---|---|
| Soluzione altamente scalabile per gestire i thin client | Gratuito fino a 10.000 dispositivi | Fino a 120.000 dispositivi                | Fino a 1 milione di dispositivi                   |
| Termini della licenza                                   | Download gratuito                  | Abbonamento per utente                    | Abbonamento per utente                            |
| Codice di licenza                                       | Non richiesto                      | Necessario                                | Necessario  |

**Tabella 1. Matrice della funzione per ciascun tipo di abbonamento (continua)**

| <b>Funzioni</b>  | <b>Wyse Management Suite Standard</b> | <b>Wyse Management Suite Pro - Private cloud</b> | <b>Wyse Management Suite Edition Pro - Cloud Edition</b> |
|--|---------------------------------------|--|--|
| Architettura   | Private cloud                         | Private cloud                                    | Public cloud   |
| Implementazione flessibile o hybrid cloud  | X                                     | √  | √  |
| Programma di installazione avanzato  | X                                     | √  | √  |
| Multi-tenancy  | X                                     | √  | √  |
| Amministrazione delegata per la granularità delle autorizzazioni                           | X                                     | √  | √  |
| Più repository per supportare l'architettura distribuita                                   | X                                     | √  | √  |
| Opzione per configurare l'alias del server Wyse Management Suite                           | X                                     | √  | √  |
| Architettura di riferimento ad alta disponibilità  | X                                     | √  | X  |
| Supporto proxy: SOCKS5 e HTTPS   | √                                     | √  | √  |
| Supporto API   | X                                     | √  | X  |
| Dell ProSupport for Software incluso   | X                                     | √  | √  |
| <b>Endpoint Dell</b>   |                                       |  |  |
| OptiPlex 7070 Ultra con Dell Hybrid Client   | X                                     | √  | √  |
| OptiPlex 3090 Ultra e 7090 Ultra con Dell Hybrid Client                                    | X                                     | √  | √  |
| Latitude 3320 con Dell Hybrid Client   | X                                     | √  | √  |
| Wyse 5070 con Dell Hybrid Client   | X                                     | √  | √  |
| Thin Client Wyse con ThinOS  | √                                     | √  | √  |
| Thin Client Wyse con ThinLinux   | √                                     | √  | √  |
| Thin Client Wyse con Windows 10 IoT Enterprise   | √                                     | √  | √  |
| Wyse PCoIP Zero Clients (firmware Teradici)  | X                                     | √  | √  |
| Software Thin Client con Wyse Converter per PC   | X                                     | √  | √  |
| <b>Reporting e monitoraggio</b>  |                                       |  |  |
| Console di gestione localizzata  | X                                     | √  | √  |
| Registri degli avvisi, degli eventi e audit log utilizzando l'applicazione e-mail e mobile | X                                     | √  | √  |
| Reporting a livello aziendale  | X                                     | √  | √  |

La tabella seguente fornisce informazioni sulle funzioni di gestione Dell Hybrid Client supportate per ciascun tipo di abbonamento.

**Tabella 2. Matrice di funzioni di gestione Dell Hybrid Client**

| <b>Funzioni di gestione Dell Hybrid Client</b>  | <b>Wyse Management Suite Standard</b> | <b>Wyse Management Suite Pro - Private cloud</b> | <b>Wyse Management Suite Edition Pro - Cloud Edition</b> |
|---|---------------------------------------|--|--|
| <b>Visibilità completa degli asset</b>  |                                       |  |  |
| Rilevamento automatico dei dispositivi  | X                                     | √  | √  |
| Gestione degli asset, dell'inventario e dei sistemi   | X                                     | √  | √  |
| Visualizzazione della configurazione valida a livello di Wyse Management Suite del dispositivo dopo l'eredità | X                                     | √  | √  |
| <b>Protezione</b>   |                                       |  |  |
| Comunicazione protetta (HTTPS)  | X                                     | √  | √  |
| MQTT sicuro   | X                                     | √  | √  |
| Autenticazione a più fattori  | X                                     | √  | √  |
| Autenticazione di Active Directory per l'amministrazione basata sui ruoli                                     | X                                     | √  | √  |
| Mapping di Active Directory tramite LDAPS   | X                                     | √  | √  |
| Single Sign-On  | X                                     | √  | √  |
| Impostazioni di blocco (attivazione/disattivazione delle porte degli endpoint supportati)                     | X                                     | √  | √  |
| <b>Gestione completa</b>  |                                       |  |  |
| Gestione delle patch e delle immagini del sistema operativo   | X                                     | √  | √  |
| Pianificazione intelligente   | X                                     | √  | √  |
| Implementazione automatica  | X                                     | √  | √  |
| Creazione di pacchetti di applicazioni per semplificare l'implementazione e ridurre al minimo i riavvii       | X                                     | √  | √  |
| Creazione e assegnazione dinamiche dei gruppi basate sugli attributi dei dispositivi                          | X                                     | √  | √  |
| Assegnazione del repository al criterio di applicazione e mappatura subnet                                    | X                                     | √  | √  |
| Gestione delle app e criteri app avanzati   | X                                     | √  | √  |
| Eredità gruppo di utenti  | X                                     | √  | √  |
| Eccezione per l'utente finale   | X                                     | √  | √  |

**Tabella 2. Matrice di funzioni di gestione Dell Hybrid Client (continua)**

| Funzioni di gestione Dell Hybrid Client   | Wyse Management Suite Standard | Wyse Management Suite Pro - Private cloud | Wyse Management Suite Edition Pro - Cloud Edition |
|---|--------------------------------|---|---|
| Annullamento automatico della registrazione dei dispositivi                                   | X                              | √   | √   |
| <b>Configurazione</b>   |                                |   |   |
| Configurazione della procedura guidata di Dell Hybrid Client                                  | X                              | √   | √   |
| Supporto per più monitor  | X                              | √   | √   |
| Profilo Follow-me   | X                              | √   | √   |
| Affiliazione di file per assegnare priorità alla modalità di distribuzione delle applicazioni | X                              | √   | √   |
| Impostazioni del BIOS e supporto alla configurazione  | X                              | √   | √   |
| Esportazione o importazione della configurazione criterio                                     | X                              | √   | √   |
| Criterio del gruppo utenti predefinito  | X                              | √   | √   |
| Configurazione del browser  | X                              | √   | √   |
| Configurare il provider di cloud  | X                              | √   | √   |
| Aggiornamento automatizzato delle applicazioni firmate da Dell                                | X                              | √   | √   |
| Roaming dei dati di personalizzazione utente  | X                              | √   | √   |
| Configurazione VNC  | X                              | √   | √   |
| Configurazione SSH  | X                              | √   | √   |

**i N.B.:** Dell Technologies consiglia di aggiornare il sistema a 12 GB di RAM, poiché è necessaria più memoria per consentire comunicazioni sicure.

**i N.B.:** Per una licenza standard, è possibile utilizzare una connessione di tipo MQTT sicuro (8443) bloccando la porta 1883 dal server Wyse Management Suite mediante Windows Firewall.

La seguente tabella fornisce informazioni sulle funzioni di gestione dei thin client Wyse e degli zero client supportate per ogni abbonamento.

**Tabella 3. Matrice di funzioni di gestione thin client e zero client Wyse**

| Funzioni di gestione thin client e zero client Wyse                                 | Wyse Management Suite Standard | Wyse Management Suite Pro - Private cloud | Wyse Management Suite Edition Pro - Cloud Edition |
|---|--------------------------------|---|---|
| <b>Visibilità completa degli asset</b>  |                                |   |   |
| Rilevamento automatico dei dispositivi  | √                              | √   | √   |
| Gestione degli asset, dell'inventario e dei sistemi                                 | √                              | √   | √   |
| Visualizzazione della configurazione valida a livello di dispositivo dopo l'eredità | √                              | √   | √   |



**Tabella 3. Matrice di funzioni di gestione thin client e zero client Wyse (continua)**

| <b>Funzioni di gestione thin client e zero client Wyse</b>  | <b>Wyse Management Suite Standard</b> | <b>Wyse Management Suite Pro - Private cloud</b> | <b>Wyse Management Suite Edition Pro - Cloud Edition</b> |
|---|---------------------------------------|--|--|
| <b>Reporting e monitoraggio</b>   |                                       |  |  |
| Shadow remoto mediante VNC  | √                                     | √  |  |
| Heartbeat configurabile e intervallo di archiviazione   | √                                     | √  | √  |
| <b>Protezione</b>   |                                       |  |  |
| Comunicazione protetta (HTTPS)  | √                                     | √  | √  |
| Implementazione del certificato 802.1x  | √                                     | √  | √  |
| MQTT sicuro   | √                                     | √  | √  |
| Autenticazione a due fattori  | X                                     | √  | √  |
| Autenticazione di Active Directory per l'amministrazione basata sui ruoli                               | X                                     | √  | √  |
| Funzionalità di aggiunta al dominio (Windows 10 IoT Enterprise)   | X                                     | √  | √  |
| Mapping di Active Directory tramite LDAPS   | X                                     | √  | √  |
| Impostazioni di blocco (attivazione o disattivazione delle porte degli endpoint supportati)             | X                                     | √  | √  |
| <b>Gestione completa</b>  |                                       |  |  |
| Gestione delle patch e delle immagini del sistema operativo   | √                                     | √  | √ **   |
| Pianificazione intelligente   | √                                     | √  | √  |
| Implementazione automatica  | √                                     | √  | √  |
| Creazione di pacchetti di applicazioni per semplificare l'implementazione e ridurre al minimo i riavvii | X                                     | √  | √  |
| Creazione e assegnazione dinamiche dei gruppi basate sugli attributi dei dispositivi                    | X                                     | √  | √  |
| Assegnazione del repository al criterio di applicazione e mappatura subnet                              | X                                     | √  | √  |
| Annullamento automatico della registrazione dei dispositivi   | √                                     | √  | √  |
| Criterio app avanzato   | X                                     | √  | √  |
| <b>Configurazione</b>   |                                       |  |  |
| Configurazione guidata Wyse ThinOS 8.x e 9.x  | √                                     | √  | √  |

**Tabella 3. Matrice di funzioni di gestione thin client e zero client Wyse (continua)**

| Funzioni di gestione thin client e zero client Wyse                                 | Wyse Management Suite Standard | Wyse Management Suite Pro - Private cloud | Wyse Management Suite Edition Pro - Cloud Edition |
|---|--------------------------------|---|---|
| Supporto per più monitor  | √                              | √   | √   |
| Wyse Easy Setup e Wyse Overlay Optimizer  | √                              | √   | √   |
| Supporto di scripting per la personalizzazione dell'installazione dell'applicazione | X                              | √   | √   |
| Impostazioni del BIOS e supporto alla configurazione                                | X                              | √   | √   |
| Esportazione/importazione della configurazione criterio                             | X                              | √   | √   |
| Supporto del pacchetto RSP  | X                              | √   | √   |
| Strumento di importazione WDM   | X                              | √   | X   |
| Eccezione per dispositivi in blocco   | X                              | √   | √   |

- i** **N.B.:** \*\* Un doppio asterisco indica che per i sistemi operativi ThinLinux e Windows 10 IoT Enterprise è necessario un repository on-premise quando si utilizza l'ambiente public cloud di Wyse Management Suite.
- i** **N.B.:** Dell Technologies consiglia di aggiornare il sistema a 12 GB di RAM, poiché è necessaria più memoria per consentire comunicazioni sicure.
- i** **N.B.:** Per una licenza standard, è possibile utilizzare una connessione di tipo MQTT sicuro (8443) bloccando la porta 1883 dal server Wyse Management Suite mediante Windows Firewall.
- i** **N.B.:** ThinOS 9.1.x, Dell Hybrid Client 1.5 e versioni successive, Wyse Device Agent 14.5.3.11 e versioni successive supportano MQTT sicuro.

# Guida introduttiva a Wyse Management Suite

Questa sezione fornisce informazioni sulle funzioni generali per iniziare ad amministrare e gestire i thin client dal software Wyse Management Suite.

## Argomenti:

- [Accesso a Wyse Management Suite su public cloud](#)
- [Prerequisiti per l'implementazione di Wyse Management Suite su private cloud](#)

## Accesso a Wyse Management Suite su public cloud

Per accedere alla console Wyse Management Suite, è necessario disporre di un web browser supportato installato nel sistema. Per accedere alla console Wyse Management Suite, procedere come segue:

1. Accedere all'edizione per public cloud (SaaS) della console Wyse Management Suite utilizzando uno dei seguenti collegamenti:
  - **Data center Stati Uniti:** [us1.wysemanagementsuite.com/ccm-web](https://us1.wysemanagementsuite.com/ccm-web)
  - **Data center UE:** [eu1.wysemanagementsuite.com/ccm-web](https://eu1.wysemanagementsuite.com/ccm-web)
2. Inserire nome utente e password.
3. Cliccare su **Accedi**.

Se si accede alla console Wyse Management Suite per la prima volta, se viene aggiunto un nuovo utente o se viene rinnovata la licenza di un utente, viene visualizzata la finestra **Termini e condizioni**. Leggere i termini e le condizioni, selezionare le rispettive caselle di controllo e cliccare su **Accetta**.

**i** **N.B.:** Si riceveranno le credenziali di accesso quando si effettua la registrazione per la versione di prova di Wyse Management Suite su [www.wysemanagementsuite.com](https://www.wysemanagementsuite.com) o quando si acquista l'abbonamento. È possibile acquistare l'abbonamento a Wyse Management Suite dal team di vendita Dell o dal partner locale di Dell. Per ulteriori informazioni, vedere [www.wysemanagementsuite.com](https://www.wysemanagementsuite.com).

**i** **N.B.:** Quando si utilizza la versione Pro di Wyse Management Suite sul public cloud, è necessario installare un repository accessibile esternamente su un server dotato di una DMZ. Inoltre, il nome di dominio completo (FQDN) del server deve essere registrato nel DNS pubblico.

## Modifica della password

Per modificare la password di accesso, procedere come segue:

1. Cliccare sul link dell'account nell'angolo superiore destro della console di gestione.
2. Cliccare su **Modifica password**.

**i** **N.B.:** Si consiglia di modificare la password dopo aver effettuato l'accesso per la prima volta. Il nome utente e la password predefiniti per altri amministratori vengono creati dal proprietario dell'account di Wyse Management Suite.

## Disconnessione

Per uscire dalla console di gestione, effettuare le seguenti operazioni:

1. Cliccare sul link dell'account nell'angolo superiore destro della console di gestione.
2. Cliccare su **Disconnetti**.

# Prerequisiti per l'implementazione di Wyse Management Suite su private cloud

Tabella 4. Prerequisiti

| Descrizione                    | Massimo 10.000 dispositivi  | Massimo 50.000 dispositivi | Massimo 120.000 dispositivi | Wyse Management Suite - Software Repository   |
|--------------------------------|---|----------------------------|-----------------------------|---|
| Sistema operativo              | Windows Server 2012 R2, Windows Server 2016 oppure Windows Server 2019 Standard. Il web server Wyse Management Suite è dotato di un web server Tomcat Apache integrato. Accertarsi di non installare i web server Microsoft IIS e Apache Tomcat separatamente.<br>Supporto linguistico: inglese, francese, italiano, tedesco, spagnolo, giapponese, cinese (versione di anteprima)  |                            |                             |   |
| Spazio minimo su disco         | 40 GB   | 120 GB                     | 200 GB                      | 120 GB  |
| Memoria minima (RAM)           | 8 GB  | 16 GB                      | 32 GB                       | 16 GB   |
| Requisiti minimi CPU           | 4   | 4                          | 16                          | 4   |
| Porte di comunicazione di rete | <p>Il programma di installazione di Wyse Management Suite aggiunge le porte TCP (Transmission Control Protocol) 443, 8080 e 1883 all'elenco delle eccezioni firewall. Le porte vengono aggiunte per accedere alla console Wyse Management Suite e per inviare le notifiche push ai thin client.</p> <ul style="list-style-type: none"> <li>● TCP 443- Comunicazione HTTPS</li> <li>● TCP 1883 - Communication MQTT</li> <li>● TCP 3306 - MariaDB (opzionale se remoto)</li> <li>● TCP 27017- MongoDB (opzionale se remoto)</li> <li>● TCP 11211 - Memcached</li> <li>● TCP 5172, 49159 - End-User Management Software Development Kit (EMSDK): opzionale e necessario solo per gestire i dispositivi Teradici</li> </ul> <p>Le porte predefinite utilizzate dal programma di installazione possono essere modificate con una porta alternativa durante l'installazione.</p> |                            |                             | <p>Il programma di installazione di Wyse Management Suite Repository aggiunge le porte TCP 443 e 8080 all'elenco delle eccezioni firewall. Le porte vengono aggiunte per accedere alle immagini del sistema operativo e alle immagini delle applicazioni che sono gestite da Wyse Management Suite.</p> |
| Browser supportati             | <p>Internet Explorer versione 11</p> <p>Google Chrome versione 58.0 e versioni successive</p> <p>Mozilla Firefox versione 52.0 e versioni successive</p> <p>Browser Edge su Windows: solo in inglese</p>  |                            |                             |   |

- Gli script di installazione e Overlay Optimizer versione 1.0 sono forniti insieme al programma di installazione di Wyse Management Suite. L'amministratore deve eseguire gli script per mettere a disposizione Overlay Optimizer in Wyse Management Suite.
- Gli script di installazione della versione 1.0 di Dell Secure Client verranno forniti insieme al programma di installazione di Wyse Management Suite. L'amministratore deve eseguire lo script per mettere a disposizione Dell Secure Client in Wyse Management Suite.
- ⓘ **N.B.:** WMS.exe e WMS\_Repo.exe devono essere installati su due server diversi. È necessario installare il repository remoto di Wyse Management Suite per il public cloud. Per il private cloud, è necessario installare il repository remoto e il repository locale di Wyse Management Suite. Il software può essere installato su una macchina fisica o virtuale. Inoltre, non è necessario che il repository del software e il server Wyse Management Suite dispongano dello stesso sistema operativo.
- ⓘ **N.B.:** Per la configurazione di 10.000 dispositivi, la memoria minima (RAM) per le comunicazioni MQTT sicure deve essere di 12 GB.
- ⓘ **N.B.:** A partire da Wyse Management Suite 3.3, è necessario utilizzare MongoDB versione 4.2.12 per le configurazioni distribuite. Non è possibile installare o aggiornare Wyse Management Suite versione 3.3 utilizzando un'altra versione del server MongoDB esterno.
- ⓘ **N.B.:** L'installazione del server e del repository di Wyse Management Suite non è supportata nei server in hosting su cloud, come Azure, Amazon Web Services e Google Cloud Platform.

# Installazione di Wyse Management Suite sul private cloud

## Prerequisiti



- Ottenere e configurare tutto l'hardware e il software richiesto. È possibile scaricare il software Wyse Management Suite da [downloads.dell.com/wyse/wms](https://downloads.dell.com/wyse/wms).
- Installare un sistema operativo server supportato su uno o più computer server.
- Accertarsi che i sistemi siano aggiornati con i service pack, le patch e gli aggiornamenti Microsoft correnti.
- Accertarsi che sia installata la versione più recente del browser supportato.
- Ottenere i diritti e le credenziali di amministratore per tutti i sistemi coinvolti nelle procedure di installazione.
- Per le funzioni Pro, ottenere una licenza valida di Wyse Management Suite. La Standard Edition non richiede una licenza.
- Accertarsi che vi sia spazio sufficiente sull'unità in cui è installato Wyse Management Suite e che il repository locale sia configurato.
- Se sono stati installati o configurati programmi antivirus o altri strumenti di monitoraggio sulla configurazione di Wyse Management Suite, Dell Technologies consiglia di disabilitare temporaneamente gli strumenti fino al completamento dell'aggiornamento. È inoltre possibile aggiungere l'esclusione appropriata per la directory di installazione, la directory temporanea e la directory del repository locale di Wyse Management Suite.

## Informazioni su questa attività


Un'installazione semplice di Wyse Management Suite è costituita dai seguenti componenti:

- Server Wyse Management Suite (include il repository per applicazioni e immagini del sistema operativo)
- Facoltativo - server di repository Wyse Management Suite aggiuntivi (repository per immagini aggiuntive, applicazioni e autenticazione AD)
- Facoltativo - Certificato HTTPS rilasciato da una CA come [www.geotrust.com/](http://www.geotrust.com/)

## Procedura

1. Cliccare due volte sul pacchetto del programma di installazione.
  2. Nella schermata **Introduzione**, cliccare su **Avanti**.  
Vengono visualizzati i dettagli dell'**EULA**.  
 **N.B.:** Questa schermata viene visualizzata solo su Wyse Management Suite versione 3.1 o versioni successive.
  3. Leggere il contratto di licenza.
  4. Selezionare la casella di controllo **Accetto i termini del contratto di licenza** e cliccare su **Avanti**.
  5. Sulla pagina **Tipo di configurazione**, selezionare i componenti da installare, quindi cliccare su **Successivo**. Le opzioni disponibili sono le seguenti:
    - Wyse Management Suite: sono disponibili due tipi di configurazione per i componenti Wyse Management Suite.
      - Tipica: richiede un'interazione minima da parte dell'utente e installa database incorporati.
      - Personalizzata: richiede delle interazioni massime da parte degli utenti ed è consigliata per utenti avanzati. Per ulteriori informazioni, vedere [Installazione personalizzata](#).
    - Teradici EM SDK: i componenti di Teradici EM SDK vengono installati come servizio.
-  **N.B.:** quando si abilita la funzione Protezione avanzata di Internet Explorer, viene visualizzata una finestra di notifica. Per disabilitare questa funzione, selezionare la casella di controllo **Disattiva la configurazione di Protezione avanzata di Internet Explorer** nella pagina **Tipo di configurazione**.


Se EM SDK è installato sul server insieme a Wyse Management Suite di un'installazione precedente, i componenti di Teradici EM SDK vengono aggiornati automaticamente.

6. Selezionare **Tipica** come **Tipo di configurazione**.
7. Inserire le nuove **Credenziali database** per i database incorporati e le nuove **Credenziali amministratore**, quindi cliccare su **Successivo**.  
 **N.B.:** le credenziali amministratore sono necessarie per eseguire l'accesso alla console web di Wyse Management Suite dopo l'installazione.

8. Nella pagina **Configurazione**, procedere come segue:




- a. Configurare la cartella condivisa e i diritti di accesso per l'utente CIFS. Le opzioni disponibili sono le seguenti:
- **Utilizza utente esistente:** selezionare questa opzione per convalidare le credenziali per un utente esistente.
  - **Crea nuovo utente:** selezionare questa opzione e inserire le credenziali per creare un nuovo utente.

La password deve contenere più di otto caratteri.

 **N.B.:** Se l'opzione **Teradici EM SDK** è abilitata nella pagina **Tipo di configurazione**, è possibile configurare la porta del server Teradici nella pagina **Configurazione**.

b. Cliccare su **Avanti**.

Viene visualizzata la schermata **Credenziali account di servizio** con le seguenti opzioni:

- **Crea nuovo utente locale:** selezionare questa opzione per immettere le credenziali e creare un nuovo utente locale con privilegi minimi. Il nuovo utente viene aggiunto al gruppo **Utenti**. Tuttavia, non disporrà dei diritti di amministratore.  
 **N.B.:** Il nome utente inserito nella schermata **Credenziali account di servizio** non deve coincidere con il nome utente Teradici. Il nome utente deve contenere da 2 a 20 caratteri. La password deve contenere da 9 a 127 caratteri e almeno un carattere maiuscolo, un carattere minuscolo, un numero e un carattere speciale. Non è consentito l'uso degli spazi per la password.
- **Utilizza un utente locale esistente:** selezionare questa opzione per immettere le credenziali di un utente locale esistente. Viene visualizzato un messaggio quando si seleziona questa opzione. Assicurarsi che l'utente esista già, che disponga dei diritti di accesso al servizio (**SeServiceLogonRight**) e che abbia eseguito correttamente l'accesso al sistema almeno una volta. Dell Technologies consiglia di assicurarsi che l'utente non disponga dei diritti di amministrazione.  
 **N.B.:** Se si seleziona questa opzione, la complessità della password non viene verificata e il nome utente immesso deve contenere da 2 a 20 caratteri.
- **Utilizza utente di dominio esistente:** selezionare questa opzione per immettere le credenziali di un utente di dominio esistente. Viene visualizzato un messaggio quando si seleziona questa opzione. Assicurarsi che l'utente esista già nel dominio, che disponga dei diritti di accesso al servizio (**SeServiceLogonRight**) e che abbia eseguito correttamente l'accesso al sistema almeno una volta. Dell Technologies consiglia di assicurarsi che l'utente non disponga dei diritti di amministrazione.  
 **N.B.:** Se si seleziona questa opzione, la complessità della password non viene verificata.

c. Cliccare su **Avanti** dopo aver inserito le credenziali.


Viene visualizzata la schermata **Credenziali Software Vault**. Software Vault viene utilizzato per archiviare i dati sensibili richiesti dall'applicazione Dell Wyse Management Suite.

d. Inserire la password per Software Vault.

La password deve contenere più di otto caratteri.

e. Cliccare su **Avanti**.

9. Accertarsi di selezionare tutte le versioni appropriate di TLS in base ai criteri di supporto dei dispositivi gestiti.

 **N.B.:** La versione di WDA precedente a WDA\_14.4.0.135\_Unified, lo strumento di importazione e l'immagine Merlin a 32 bit non sono compatibili con TLSv1.1 e versioni successive. Selezionare TLSv1.0 se l'ambiente Wyse Management Suite ha dispositivi con versione precedente di WDA, lo strumento di importazione o dispositivi installati con un'immagine Merlin a 32 bit.

10. Accedere alla posizione in cui si desidera installare il software e al repository dei file tenant locale, quindi cliccare su **Successivo**.

Il percorso predefinito della cartella di destinazione per installare il software è `C:\Program Files\DELL\WMS`.

11. Cliccare su **Avanti**.

Viene visualizzata la pagina **Riepilogo pre-installazione**.

12. Cliccare su **Avanti** per installare il software.

Il programma di installazione impiega circa 4-5 minuti per completare l'installazione. Tuttavia, se i componenti dipendenti, come runtime VC, non sono installati nel sistema, potrebbe richiedere più tempo.

13. Cliccare su **Avvia** per aprire la console web di Wyse Management Suite.

14. Nella console web, cliccare su **Per iniziare**.

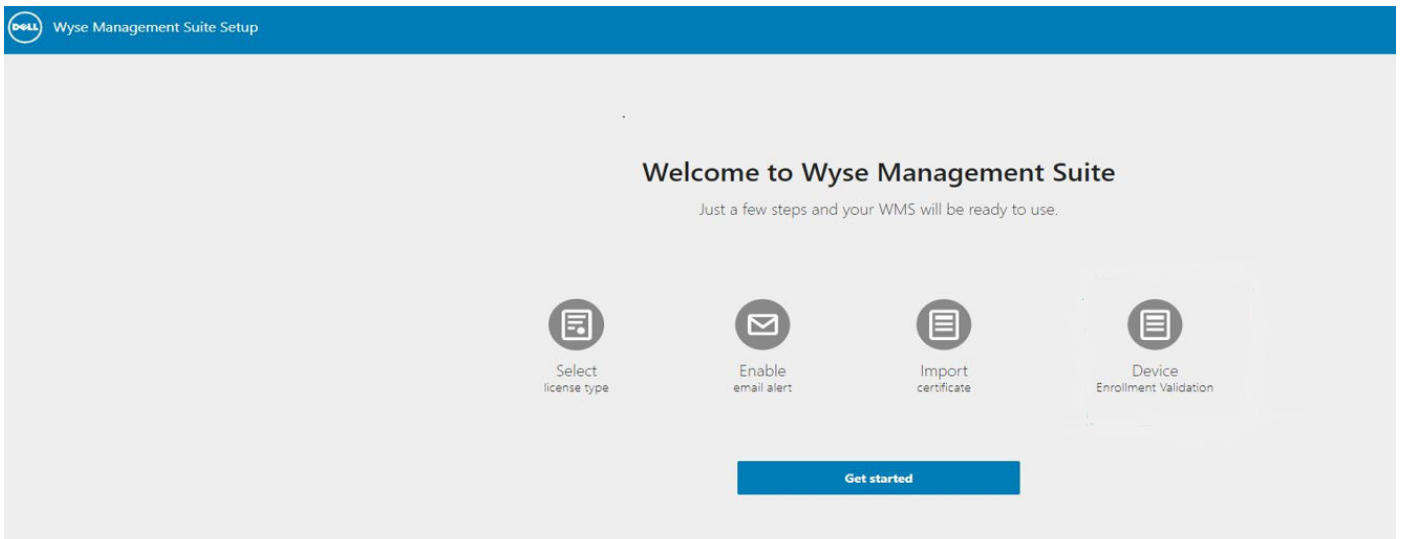


Figura 1. Pagina Introduzione

15. Selezionare la licenza preferita.

- Se si seleziona il tipo di licenza **Standard**, cliccare su **Successivo** per procedere con l'installazione standard di Wyse Management Suite.
- Se si seleziona il tipo di licenza **Pro**, è necessario importare una licenza Wyse Management Suite valida. Per importare la licenza Wyse Management Suite, inserire le informazioni richieste per importare la licenza se il server dispone di una connettività Internet. Inoltre, è possibile generare il codice di licenza effettuando l'accesso al portale public cloud di Wyse Management Suite e inserendo la chiave nel campo del codice di licenza.

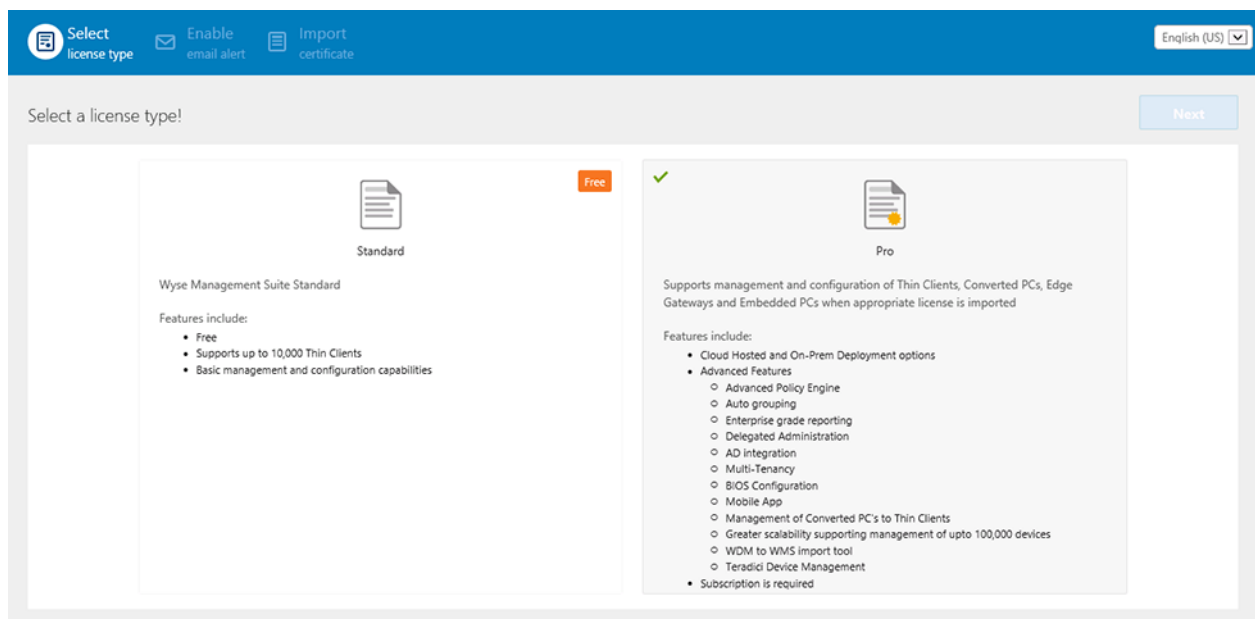


Figura 2. Tipo di licenza

Enter license information ?

Enter your credentials to import licensing information ?

Username john\_smith

Password password

Data center -- select a data center --

Number of TC seats ?

Number of Edge Gateway & Embedded PC seats ?

Number of Wyse Software Thin Client seats ?

Number of Hybrid Client seats ?

Import

OR

Input your WMS Pro license key

License Key ?

Import

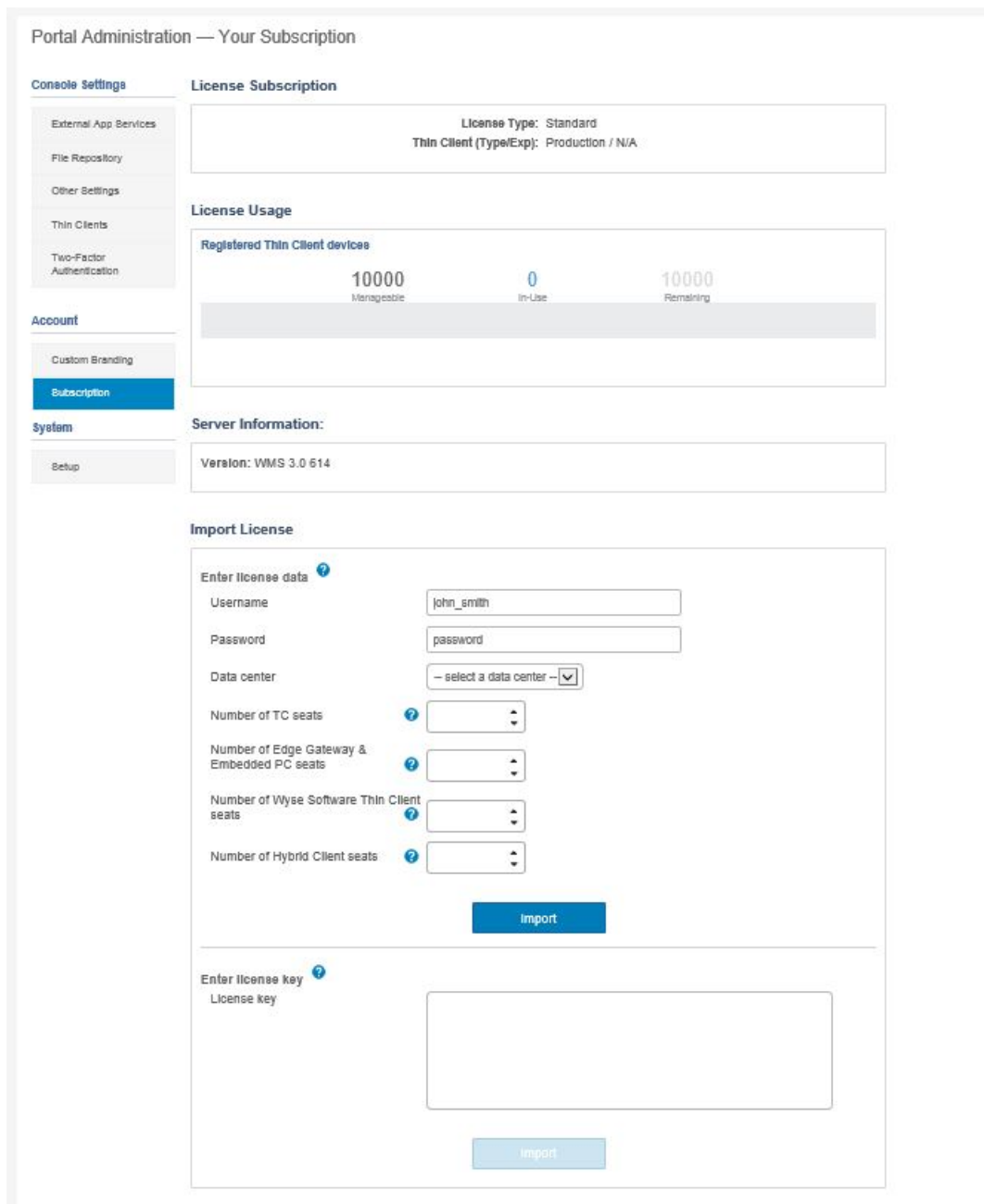
Activate Windows  
Go to System in Control Panel to activate Wii

**Figura 3. Informazioni sulla licenza**

Per esportare un codice di licenza dal portale cloud Wyse Management Suite, effettuare le operazioni riportate di seguito:

- a. Accedere al portale cloud di Wyse Management Suite utilizzando uno dei seguenti collegamenti:
  - Data center Stati Uniti: [us1.wysemanagementsuite.com/ccm-web](https://us1.wysemanagementsuite.com/ccm-web)
  - Data center UE: [eu1.wysemanagementsuite.com/ccm-web](https://eu1.wysemanagementsuite.com/ccm-web)
- b. Andare a **Amministrazione portale > Abbonamento**.





**Figura 4. Amministratore portale**

- c. Inserire il numero di utenze thin client.
- d. Cliccare su **Esporta**.

Per esportare la licenza, selezionare **WMS 1.1** o **WMS 1.0** dall'elenco a discesa.

Nella pagina di riepilogo vengono mostrati i dettagli della licenza dopo l'importazione.

- 16. Inserire le informazioni del server SMTP e cliccare su **Salva**.

**i** **N.B.:** è possibile ignorare questa schermata e apportare modifiche nella console in un secondo momento.

Figura 5. Avviso e-mail

**N.B.:** è necessario inserire informazioni valide relative al server SMTP per ricevere notifiche e-mail da Wyse Management Suite.

17. Importare il certificato SSL per proteggere le comunicazioni con il server Wyse Management Suite. Inserire il certificato pubblico, privato e Apache e cliccare sul pulsante **Importa**. L'importazione del certificato richiede tre minuti per configurare e riavviare i servizi Tomcat. È possibile ignorare questa schermata e completare la configurazione o apportare modifiche in un secondo momento nella console, effettuando l'accesso al private cloud di Wyse Management Suite ed effettuando importazioni dalla pagina **Amministrazione portale**.

**N.B.:**

Per impostazione predefinita, Wyse Management Suite importa il certificato SSL con firma automatica che viene generato durante l'installazione per proteggere le comunicazioni tra il client e il server Wyse Management Suite. Se non si importare un certificato valido per il server Wyse Management Suite, quando si accede a Wyse Management Suite da un computer diverso da quello in cui è installato il server, viene visualizzato un messaggio di avviso. Questo messaggio di avviso viene visualizzato in quanto il certificato con firma automatica generato durante l'installazione non è firmato da una CA come [geotrust.com](http://geotrust.com). È possibile importare un certificato .pem o .pfx.

Figura 6. Coppia di valori chiave o certificato

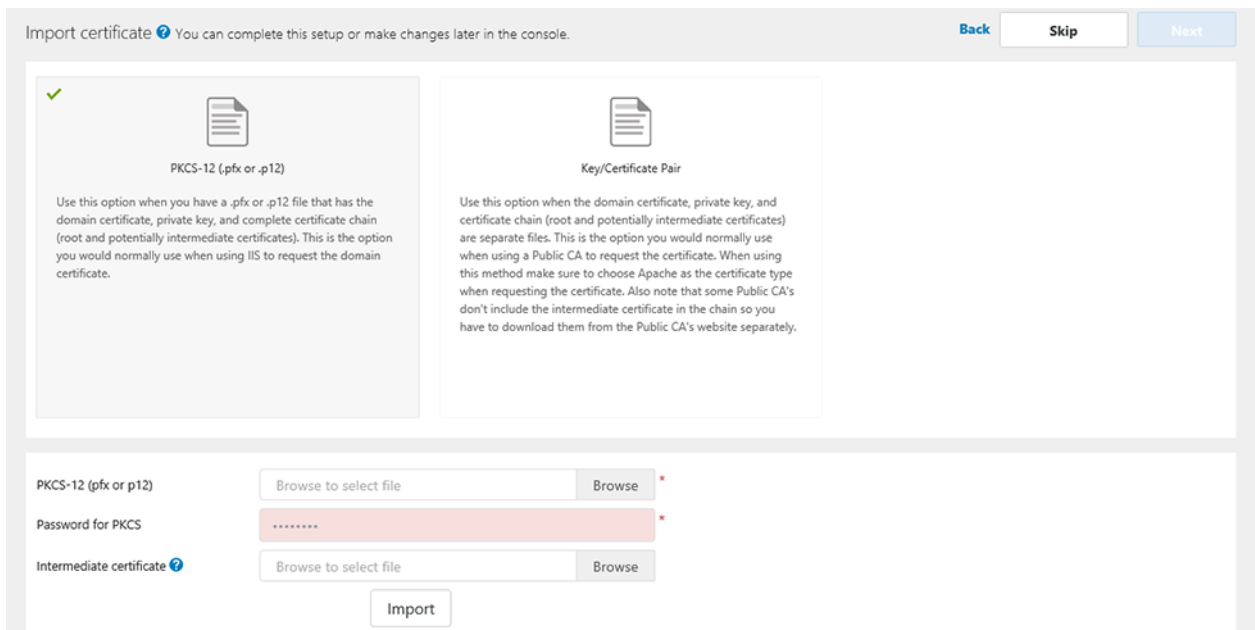


Figura 7. PKCS-12

- Nella pagina **Dispositivo**, è possibile abilitare **Convalida iscrizione** per consentire agli amministratori di controllare la registrazione manuale e automatica dei thin client a un gruppo.

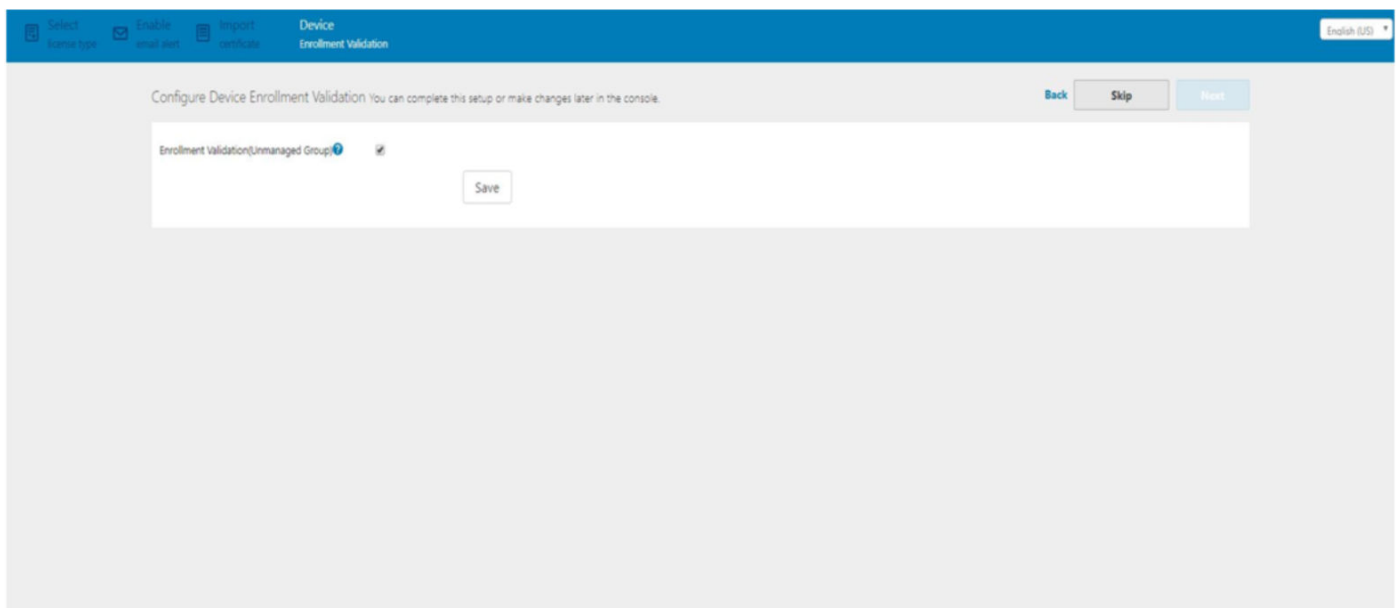


Figura 8. Convalida iscrizione

- Cliccare su **Salva**, quindi su **Successivo**.
- Cliccare su **Accedi a WMS**.  
Viene visualizzata la pagina di accesso **Dell Management Portal**.

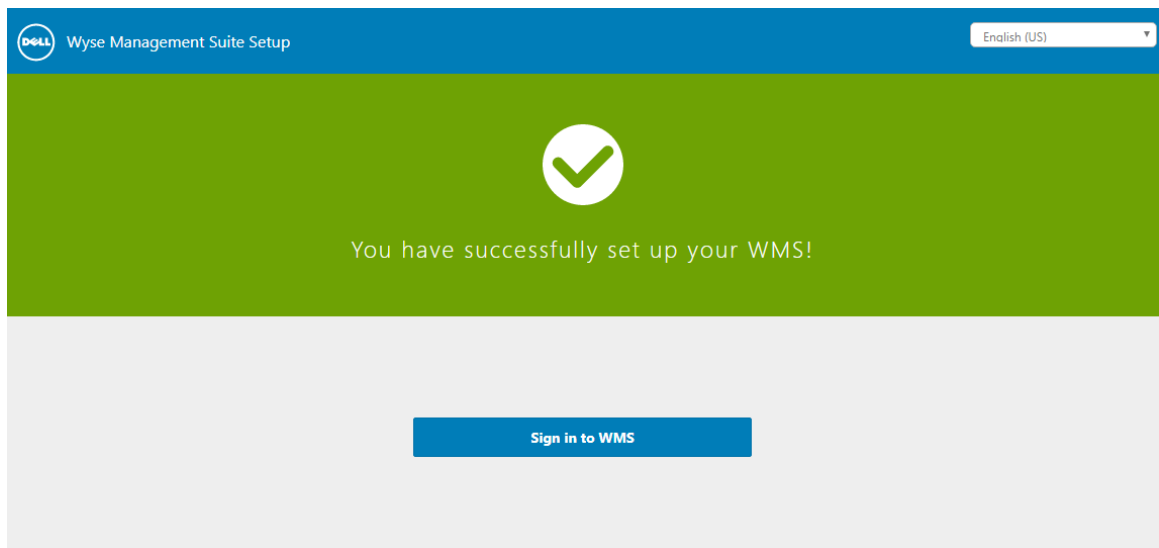


Figura 9. Pagina Accedi

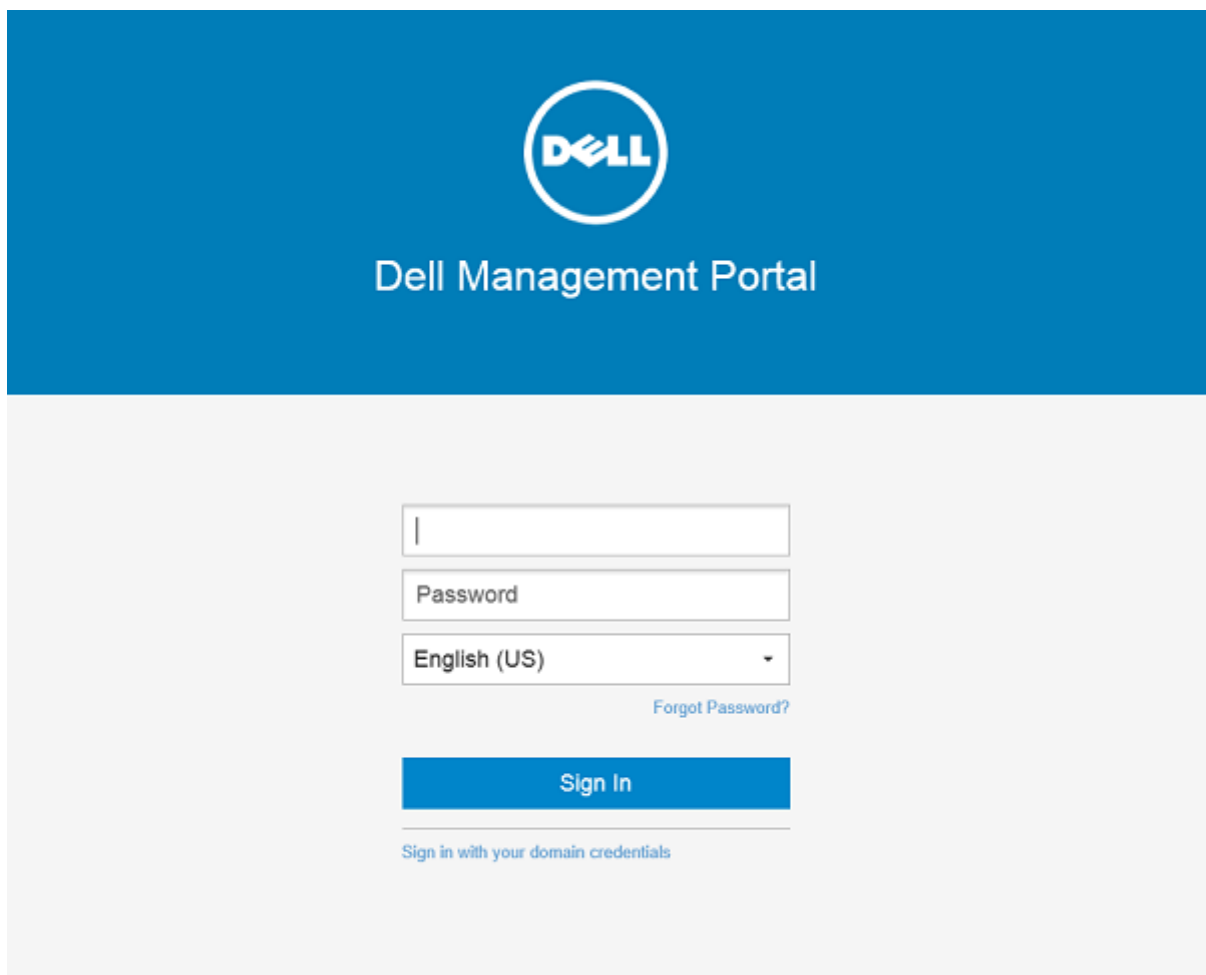



Figura 10. Dell Management Portal

 **N.B.:** le licenze possono essere aggiornate o estese in un secondo momento dalla pagina **Amministrazione portale**.

#### Argomenti:

- [Accesso a Wyse Management Suite](#)
- [Aree funzionali della console di gestione](#)
- [Configurazione e gestione dei thin client](#)
- [Creazione del gruppo di criteri e aggiornamento della configurazione](#)
- [Registrazione del nuovo thin client](#)

## Accesso a Wyse Management Suite

### Informazioni su questa attività

Per accedere alla console di gestione, effettuare le seguenti operazioni:

#### Procedura

1. Se si utilizza Internet Explorer, disabilitare le impostazioni **Protezione avanzata Internet Explorer** e **Visualizzazione compatibilità**
2. Utilizzare un web browser supportato su qualsiasi computer con accesso a Internet e accedere alla versione del private cloud di Wyse Management Suite da <https://<FQDN>/ccm-web>. Ad esempio, <https://wmserver.domain.com/ccm-web>, dove [wmserver.domain.com](https://wmserver.domain.com) è il nome di dominio completo del server.
3. Immettere il nome utente e la password.
4. Cliccare su **Accedi**

## Aree funzionali della console di gestione

La console Wyse Management Suite è organizzata nelle seguenti aree funzionali:

### Informazioni su questa attività

- La pagina **Dashboard** fornisce informazioni relative a ciascuna area funzionale del sistema.
- La pagina **Gruppi e configurazioni** impiega una gestione criteri di gruppo gerarchica gestione criteri di gruppo per la configurazione dei dispositivi. Se lo si desidera, è possibile creare dei sottogruppi dei criteri di gruppo globali per classificare i dispositivi in base a standard aziendali. Ad esempio, è possibile raggruppare i dispositivi in base alle funzioni di processo, al tipo di dispositivo, BYOD e così via.
- La pagina **Dispositivi** consente di visualizzare e gestire dispositivi, tipi di dispositivi, dispositivi e configurazioni specifiche del dispositivo.
- La pagina **App e dati** fornisce la gestione di applicazioni dispositivo, immagini del sistema operativo, criteri, file certificato, loghi e immagini di sfondo.
- La pagina **Regole** consente di aggiungere, modificare e attivare o disattivare regole come il raggruppamento automatico e le notifiche avvisi.
- La pagina **Processi** consente di creare processi per attività quali riavvio, WOL e criteri applicazioni o immagine che è necessario distribuire sui dispositivi registrati.
- La pagina **Eventi** consente di visualizzare e verificare eventi di sistema e avvisi.
- La pagina **Utenti** consente di assegnare agli utenti locali e a quelli importati da Active Directory i ruoli di amministratore globale, amministratore di gruppo e visualizzatore per accedere a Wyse Management Suite. Agli utenti vengono assegnate autorizzazioni per eseguire operazioni in base ai ruoli loro assegnati.
- La pagina **Amministrazione portale** consente agli amministratori di configurare varie impostazioni di sistema, come configurazione del repository locale, sottoscrizione licenza, configurazione di Active Directory e autenticazione a due fattori. Per maggiori informazioni, consultare la *Guida dell'amministratore di Dell Wyse Management Suite* all'indirizzo [support.dell.com](http://support.dell.com).

## Configurazione e gestione dei thin client

**Gestione della configurazione:** Wyse Management Suite supporta una gerarchia di gruppi e sottogruppi. I gruppi possono essere creati manualmente o automaticamente in base a regole definite dall'amministratore di sistema. È possibile organizzare in base ai gruppi funzionali, ad esempio, marketing, vendite e progettazione o in base alla gerarchia di posizione, ad esempio paese, stato e città.

**i N.B.:**

Nella Pro Edition, gli amministratori di sistema possono aggiungere regole per creare gruppi. Inoltre possono assegnare i dispositivi a un gruppo esistente a seconda degli attributi del dispositivo, come subnet, fuso orario e posizione.

È inoltre possibile configurare quanto segue:

- Impostazioni o criteri che si applicano a tutti i dispositivi nell'account tenant che sono impostati nel Gruppo con criteri predefiniti. Tali impostazioni e criteri sono la serie globale di parametri da cui ereditano tutti i gruppi e i sottogruppi.
- Le impostazioni o i parametri che sono configurati nei gruppi di livello inferiore hanno la precedenza sulle impostazioni che sono state configurate nei gruppi padre o di livello superiore.
- Parametri che sono specifici di un determinato dispositivo che possono essere configurati dalla pagina **Dettagli dispositivo**. Questi parametri, come i gruppi di livello inferiore, hanno la precedenza sulle impostazioni configurate nei gruppi di livello superiore.

I parametri di configurazione vengono distribuiti su tutti i dispositivi di un determinato gruppo e in tutti i sottogruppi, quando l'amministratore crea e pubblica il criterio.

Dopo che una configurazione viene pubblicata e propagata ai dispositivi, le impostazioni non vengono inviate nuovamente ai dispositivi fino a quando l'amministratore non effettua una modifica. I nuovi dispositivi che vengono registrati, ricevono il criterio di configurazione valido per il gruppo in cui sono stati registrati. Sono inclusi i parametri ereditati dal gruppo globale e dai gruppi di livello intermedio.

I criteri di configurazione vengono pubblicati immediatamente e non possono essere pianificati per un secondo momento. Un piccolo numero di modifiche dei criteri, ad esempio le impostazioni dello schermo, può forzare un riavvio.

**Implementazione delle applicazioni e dell'immagine del sistema operativo:** gli aggiornamenti relativi ad applicazioni e immagini del sistema operativo possono essere implementate dalla scheda **App e dati**. Le applicazioni vengono implementate in base ai gruppi di criteri.

**i N.B.:** il criterio di applicazione avanzato consente di distribuire un'applicazione al gruppo corrente e a tutti i sottogruppi in base alle esigenze. Le immagini del sistema operativo possono essere distribuite soltanto nel gruppo corrente.

Wyse Management Suite supporta criteri di applicazione standard e avanzati. Un criterio di applicazione standard consente di installare un singolo pacchetto di applicazione. È necessario riavviare il dispositivo prima e dopo ogni installazione di applicazione. Con un criterio di applicazione avanzato, è possibile installare più pacchetti di applicazione solo con due riavvii. Questa funzione è disponibile solo nella Pro Edition. I criteri di applicazione avanzati inoltre supportano l'esecuzione di script pre e post-installazione che potrebbero essere necessari per l'installazione di una particolare applicazione.

È possibile configurare criteri di applicazione standard e avanzati in modo che vengano applicati automaticamente quando o un dispositivo viene registrato con Wyse Management Suite o quando un dispositivo viene spostato in un nuovo gruppo.

L'implementazione dei criteri di applicazione e delle immagini del sistema operativo nei thin client può essere programmata in modo da essere eseguita immediatamente o in base al fuso orario del dispositivo o qualsiasi altro fuso orario specificato.

**Inventario dei dispositivi:** questa opzione può essere individuata facendo clic sulla scheda **Dispositivi**. Per impostazione predefinita, questa opzione consente di visualizzare un elenco impaginato di tutti i dispositivi presenti del sistema. L'amministratore può scegliere di visualizzare un sottoinsieme di dispositivi utilizzando vari criteri filtro, quali gruppi o sottogruppi, tipo di dispositivo, tipo di sistema operativo, stato, subnet e piattaforma o fuso orario.

Per andare alla pagina **Dettagli dispositivo** per un determinato dispositivo, fare clic sulla voce del dispositivo elencata in questa pagina. Vengono visualizzati tutti i dettagli del dispositivo.

La pagina **Dettagli dispositivo** inoltre visualizza tutti i parametri di configurazione applicabili a tale dispositivo insieme al livello di gruppo al quale viene applicato ciascun parametro.

Questa pagina consente inoltre agli amministratori di impostare i parametri di configurazione specifici di un determinato dispositivo, attivando il pulsante **Eccezioni dispositivo**. I parametri configurati in questa sezione escludono eventuali parametri configurati nei gruppi e/o a livello globale.

**Report:** gli amministratori possono generare e visualizzare report preconfezionati basati su filtri predefiniti. Per generare dei report preconfezionati, fare clic sulla scheda **Report** della pagina **Amministrazione portale**

**Applicazione mobile:** l'amministratore può ricevere notifiche di avviso e gestire i dispositivi utilizzando l'applicazione mobile disponibile per i dispositivi Android. Per scaricare l'applicazione mobile e la guida introduttiva, fare clic sulla scheda **Avvisi e classificazione** nella pagina **Amministrazione portale**.

# Creazione del gruppo di criteri e aggiornamento della configurazione

Per creare un criterio e aggiornare la configurazione, effettuare le seguenti operazioni:

1. Accedere come amministratore.
2. Per creare un gruppo di criteri, effettuare le seguenti operazioni:
  - a. Selezionare **Gruppi e configurazioni**, quindi fare clic sul pulsante **+** nel riquadro di sinistra.
  - b. Immettere il nome del gruppo e la descrizione.
  - c. Selezionare la casella di controllo **Abilitato**.
  - d. Immettere il token di gruppo.
  - e. Fare clic su **Salva**.
3. Per aggiornare o modificare un gruppo di criteri, effettuare le seguenti operazioni:
  - a. Fare clic su **Modifica criteri** e selezionare il sistema operativo che il criterio deve gestire.
  - b. Selezionare i criteri da modificare e completare la configurazione.
  - c. Fare clic su **Salva e pubblica**.

## **N.B.:**

- Per ulteriori dettagli sui diversi criteri di configurazione supportati da Wyse Management Suite, vedere la *Guida dell'amministratore di Dell Wyse Management Suite* all'indirizzo [support.dell.com](http://support.dell.com).
- È possibile creare una regola per creare automaticamente un gruppo e/o assegnare un dispositivo a un gruppo in base a specifici attributi quali subnet, fuso orario e posizione.

## Registrazione del nuovo thin client

 **N.B.:** Per informazioni sull'ambiente di sicurezza del cliente, vedere [Wyse Device Agent](#).

È possibile registrare manualmente un thin client con Wyse Management Suite tramite il Wyse Device Agent (WDA). È inoltre possibile registrare un thin client automaticamente configurando i tag di opzione appropriati sul server DHCP o configurando i record DNS SRV appropriati sul server DNS.

Se si desidera che i dispositivi in subnet diverse effettuino l'accesso automaticamente a gruppi differenti di Wyse Management Suite con più subnet, utilizzare i tag di opzione DHCP per registrare un thin client. Ad esempio, i dispositivi in TimeZone\_A possono eseguire l'accesso al gruppo ProfileGroup configurato per TimeZoneA.

Se si desidera immettere le informazioni relative al server Wyse Management Suite in TLD e se è stato installato Wyse Management Suite Pro per consentire l'assegnazione automatica dei gruppi basata sulle regole dispositivo, utilizzare i record DNS SRV record sul server DNS per effettuare la registrazione di un thin client. Ad esempio, se il dispositivo effettua l'accesso da TimeZoneA, assegnarlo al gruppo ProfileGroup configurato per TimeZoneA.

Per Wyse Management Suite su un cloud privato con certificati autofirmati, i thin client devono disporre delle seguenti versioni di Wyse Device Agents o firmware installato per la comunicazione protetta:

- Windows sistemi Embedded: 13.0 o versioni successive
- Thin Linux: 2.0.24 o versioni successive
- ThinOS: firmware 8.4 o versioni successive
- È possibile registrare un dispositivo con una versione precedente dell'agente utilizzando l'URL HTTP invece di HTTPS. Dopo aver aggiornato l'agente o il firmware alla versione più recente, la comunicazione con Wyse Management Suite passa automaticamente ad https.
- È possibile scaricare la versione più recente di WDA su [downloads.dell.com/wyse/wda](http://downloads.dell.com/wyse/wda).
- Per Wyse Management Suite installato in un cloud privato, andare ad **Amministrazione portale > Configurazione** e selezionare la casella di controllo **Convalida certificato**, se sono stati importati i certificati da un'autorità di certificazione, ad esempio [www.geotrust.com](http://www.geotrust.com). Questa casella di controllo non deve essere selezionata se i certificati non sono stati importati da un'autorità

di certificazione nota. Questa opzione non è disponibile per Wyse Management Suite in un cloud pubblico in quanto la convalida del certificato in un cloud pubblico è sempre abilitata.

## Registrazione manuale del dispositivo ThinOS

Per registrare manualmente i dispositivi ThinOS, effettuare le seguenti operazioni:

### Procedura

1. Dal menu del desktop, andare a **Configurazione del sistema Configurazione centrale**. Viene visualizzata la finestra **Configurazione centrale**.

2. Cliccare sulla scheda **WDA**.

L'opzione **WMS** è selezionata per impostazione predefinita.

**N.B.:** il servizio WDA si esegue automaticamente dopo il completamento del processo di avvio del client.

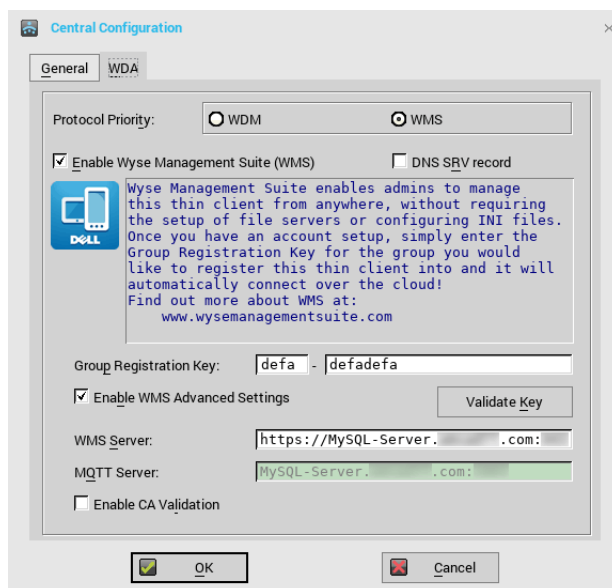


Figura 11. Configurazione centrale

3. Selezionare la casella di controllo **Abilita Wyse Management Suite** per abilitare Wyse Management Suite.

4. Inserire il **Codice di registrazione gruppo** come configurato dall'amministratore per il gruppo desiderato.

5. Selezionare l'opzione **Abilita impostazioni avanzate WMS**, quindi immettere i dettagli del server WMS o MQTT.

6. Abilitare o disabilitare la convalida CA in base al tipo di licenza: public cloud o private cloud.

- Public cloud: selezionare la casella di controllo **Abilita convalida CA** se il dispositivo è registrato con Wyse Management Suite nel public cloud.
- Private cloud: selezionare la casella di controllo **Abilita convalida CA** se sono stati importati i certificati da un'autorità di certificazione nota al proprio server Wyse Management Suite.

**N.B.:**

Per la versione cloud Pro di Wyse Management Suite negli Stati Uniti, non modificare i dettagli del server WMS e del server MQTT predefiniti. Per la versione cloud Pro di Wyse Management Suite in Europa, utilizzare i seguenti dati:

- Server CCM: [eu1.wysemanagementsuite.com](https://eu1.wysemanagementsuite.com)
- Server MQTT: [eu1-pns.wysemanagementsuite.com:1883](https://eu1-pns.wysemanagementsuite.com:1883)

7. Per verificare la configurazione, cliccare su **Convalida codice**. Il dispositivo si riavvia automaticamente dopo la convalida del codice.

**N.B.:** se il codice non viene convalidato, verificare le credenziali fornite. Accertarsi che le porte 443 e 1883 non siano bloccate dalla rete.

8. Cliccare su **OK**.



Il dispositivo viene registrato nella console Wyse Management Suite.

### Fasi successive

Per informazioni su come registrare i dispositivi Windows Embedded Standard e i dispositivi Linux, consultare [Registrazione manuale dei dispositivi Windows Embedded](#) e [Registrazione manuale dei dispositivi Linux](#).

## Registrazione dei dispositivi ThinOS mediante i file INI

Se si desidera configurare i dispositivi ThinOS utilizzando wnos.ini o xen.ini, è possibile pubblicare ulteriori informazioni nei file .ini per informare i dispositivi di accedere a un server Wyse Management Suite.

Esempi:

- Esempio per ThinOS 8.5:

```
WDAService=yes \  
Priority=WMS \  
WMSEnable=yes \  
Server= <URL del server> \  
CAValidation=no \  
Override=yes
```

- Esempio per ThinOS 8.4:

```
WDAService=yes \  
Priority=CCM \  
CCMEnable=yes \  
CCMServer=<URL del server> \  
GroupPrefix=< Prefisso > \  
GroupKey=< Chiave > \  
MQTTServer=<URL del server> \  
Override=yes \  
CAValidation=no
```

Per ulteriori informazioni, consultare la versione più recente della *Guida di Dell Wyse ThinOS INI* all'indirizzo [support.dell.com](http://support.dell.com).

### N.B.:

- Per ThinOS 8.3 (ThinOS Lite 2.3) e versioni successive, un comando `WDA Service Priority` consente di specificare il protocollo di gestione. Tale comando viene utilizzato per individuare il server di gestione.
- I tag CCM per la versione ThinOS 8.3, 8.4 e 8.5 sono diversi.

## Registrazione dei dispositivi mediante i tag di opzione DHCP

### N.B.:

- Per istruzioni dettagliate su come aggiungere i tag opzione DHCP sul server Windows, vedere [Creazione e configurazione dei tag opzione DHCP](#). Per informazioni sull'ambiente di sicurezza del cliente, vedere [Wyse Device Agent](#).

È possibile registrare i dispositivi utilizzando i seguenti tag opzione DHCP:

**Tabella 5. Registrazione dei dispositivi mediante i tag di opzione DHCP**

| Tag opzione                                      | Descrizione  |
|--|--|
| <b>Nome:</b> WMS<br><b>Tipo di dati:</b> stringa | Questo tag punta all'URL del server Wyse Management Suite. Ad esempio, <code>wmserver.acme.com:443</code> , dove <code>wmserver.acme.com</code> è il nome di dominio completo del server in cui è installato Wyse Management Suite. Per i collegamenti |

**Tabella 5. Registrazione dei dispositivi mediante i tag di opzione DHCP (continua)**

| Tag opzione  | Descrizione  |
|--|--|
| <p><b>Codice:</b> 165</p> <p><b>Descrizione:</b> FQDN server WMS</p>   | <p>per registrare i dispositivi nel public cloud di Wyse Management Suite, vedere <a href="#">Guida introduttiva a Wyse Management Suite su public cloud</a>.</p> <p><b>N.B.:</b> non utilizzare https:// nell'URL del server, altrimenti il thin client non verrà registrato in Wyse Management Suite. Utilizzare https:// se non è possibile registrare il dispositivo ThinOS 9.x in Wyse Management Suite.</p>  |
| <p><b>Nome:</b> MQTT</p> <p><b>Tipo di dati:</b> stringa</p> <p><b>Codice:</b> 166</p> <p><b>Descrizione:</b> server MQTT</p>                                  | <p>Questo tag indirizza il dispositivo al server PNS Wyse Management Suite. Per l'installazione nel private cloud, il dispositivo viene indirizzato al servizio MQTT sul server Wyse Management Suite. Ad esempio, <code>wmsservername.domain.com:1883</code>.</p> <p>Per registrare i dispositivi nel public cloud di Wyse Management Suite, il dispositivo deve puntare ai server PNS (MQTT) nel public cloud. Per esempio:</p> <p>US1:<a href="https://us1-pns.wysemanagementsuite.com">us1-pns.wysemanagementsuite.com</a></p> <p>EU1:<a href="https://eu1-pns.wysemanagementsuite.com">eu1-pns.wysemanagementsuite.com</a></p> <p>È necessario inserire i dettagli del server MQTT quando si configurano i dettagli di Wyse Device Agent nella versione precedente dei dispositivi ThinOS e Windows Embedded. MQTT è un componente di WMS richiesto per inviare notifiche ai thin client. Gli URL, con e senza dettagli MQTT, devono essere aggiunti all'elenco dei consentiti nell'ambiente public cloud di Wyse Management Suite.</p> <p><b>N.B.:</b> Non è possibile utilizzare gli URL MQTT per accedere a Wyse Management Suite.</p> |
| <p><b>Nome:</b> convalida CA</p> <p><b>Tipo di dati:</b> stringa</p> <p><b>Codice:</b> 167</p> <p><b>Descrizione:</b> convalida autorità di certificazione</p> | <p>Questo tag è richiesto se Wyse Management Suite è installato sul sistema nel private cloud. Non aggiungere questo tag opzione se i dispositivi vengono registrati con Wyse Management Suite nel public cloud.</p> <p>Inserire <b>True</b> se i certificati SSL sono stati importati da un'autorità nota per la comunicazione https tra il client e il server Wyse Management Suite.</p> <p>Inserire <b>False</b> se i certificati SSL non sono stati importati da un'autorità nota per la comunicazione https tra il client e il server Wyse Management Suite.</p>  |
| <p><b>Nome:</b> GroupToken</p> <p><b>Tipo di dati:</b> stringa</p> <p><b>Codice:</b> 199</p> <p><b>Descrizione:</b> token di gruppo</p>                        | <p>Questo tag è richiesto per registrare i dispositivi ThinOS con Wyse Management Suite su private o public cloud.</p> <p>Questo tag è opzionale per registrare i dispositivi Windows Embedded Standard o ThinLinux con Wyse Management Suite su private cloud. Se il tag non è disponibile, i dispositivi vengono registrati automaticamente nel gruppo non gestito durante l'installazione in loco.</p>  |

## Registrazione dei dispositivi mediante il record DNS SRV

**N.B.:** Per informazioni sull'ambiente di sicurezza del cliente, vedere [Wyse Device Agent](#).

La registrazione dei dispositivi DNS è supportata con le seguenti versioni di Wyse Device Agent:

- Windows sistemi Embedded: 13.0 o versioni successive
- Thin Linux: 2.0.24 o versioni successive
- ThinOS: firmware 8.4 o versioni successive

Se i campi del record SRV DNS sono impostati con valori validi, è possibile registrare i dispositivi con il server Wyse Management Suite.


**N.B.:** per istruzioni dettagliate su come aggiungere record SRV DNS al server Windows, vedere [Creazione e configurazione dei record SRV DNS](#).

La tabella seguente elenca i valori validi per i record SRV DNS:

**Tabella 6. Configurazione dei dispositivi mediante il record SRV DNS**

| URL/tag  | Descrizione   |
|--|---|
| <p><b>Nome record</b> - _WMS_MGMT</p> <p><b>FQDN record</b> - _WMS_MGMT._tcp. &lt;nomedidominio&gt;</p> <p><b>Tipo di record</b> - SRV</p>       | <p>Questo record punta all'URL del server Wyse Management Suite. Ad esempio, <code>wmserver.acme.com:443</code>, dove <code>wmserver.acme.com</code> è il nome di dominio completo del server in cui è installato Wyse Management Suite. Per i collegamenti per registrare i dispositivi nel public cloud di Wyse Management Suite, vedere <a href="#">Guida introduttiva a Wyse Management Suite su public cloud</a>.</p> <p><b>N.B.:</b> non utilizzare <code>https://</code> nell'URL del server, altrimenti il thin client non verrà registrato in Wyse Management Suite. Utilizzare <code>https://</code> se non è possibile registrare il dispositivo ThinOS 9.x in Wyse Management Suite.</p>  |
| <p><b>Nome record</b> - _WMS_MQTT</p> <p><b>FQDN record</b> - _WMS_MQTT._tcp. &lt;nomedidominio&gt;</p> <p><b>Tipo di record</b> - SRV</p>       | <p>Questo record indirizza il dispositivo al server PNS Wyse Management Suite. Per l'installazione nel private cloud, il dispositivo viene indirizzato al servizio MQTT sul server Wyse Management Suite. Ad esempio, <code>wmservername.domain.com:1883</code>.</p> <p><b>N.B.:</b> MQTT è opzionale per la versione più recente di Wyse Management Suite.</p> <p>Per registrare i dispositivi nel public cloud di Wyse Management Suite, il dispositivo deve puntare ai server PNS (MQTT) nel public cloud. Per esempio:</p> <p>US1—<a href="#">us1-pns.wysemanagementsuite.com</a></p> <p>EU1—<a href="#">eu1-pns.wysemanagementsuite.com</a></p> <p>È necessario inserire i dettagli del server MQTT quando si configurano i dettagli di Wyse Device Agent nella versione precedente dei dispositivi ThinOS e Windows Embedded. MQTT è un componente di WMS richiesto per inviare notifiche ai thin client. Gli URL, con e senza dettagli MQTT, devono essere aggiunti all'elenco dei consentiti nell'ambiente public cloud di Wyse Management Suite.</p> <p><b>N.B.:</b> Non è possibile utilizzare gli URL MQTT per accedere a Wyse Management Suite.</p> |
| <p><b>Nome record</b> - _WMS_GROUPTOKEN</p> <p><b>FQDN record</b> - _WMS_GROUPTOKEN.&lt;dominio&gt;</p> <p><b>Tipo di record</b> - TESTO</p>     | <p>Questo record è necessario per registrare i dispositivi ThinOS con Wyse Management Suite su private o public cloud.</p> <p>Questo record è opzionale per registrare i dispositivi Windows Embedded Standard o ThinLinux con Wyse Management Suite sul private cloud. Se il record non è disponibile, i dispositivi vengono registrati automaticamente nel gruppo non gestito durante l'installazione on-premise.</p> <p><b>N.B.:</b> token di gruppo è opzionale per la versione più recente di Wyse Management Suite per il private cloud.</p>  |
| <p><b>Nome record</b> - _WMS_CAVALIDATION</p> <p><b>FQDN record</b> - _WMS_CAVALIDATION.&lt;dominio&gt;</p> <p><b>Tipo di record</b> - TESTO</p> | <p>Questo record è necessario se Wyse Management Suite è installato sul sistema nel private cloud. Non aggiungere questo record opzionale se si sta registrando i dispositivi con Wyse Management Suite sul public cloud.</p> <p>Inserire <b>True</b> se i certificati SSL sono stati importati da un'autorità nota per la comunicazione https tra il client e il server Wyse Management Suite.</p>   |

**Tabella 6. Configurazione dei dispositivi mediante il record SRV DNS (continua)**

| URL/tag | Descrizione   |
|---------|---|
|         | Inserire <b>False</b> se i certificati SSL non sono stati importati da un'autorità nota per la comunicazione https tra il client e il server Wyse Management Suite.<br> <b>N.B.:</b> la convalida CA è opzionale per la versione più recente di Wyse Management Suite. |

## Registrazione dei dispositivi mediante i campi del record DNS protetto o le opzioni di ambito DHCP protetto

A partire da Wyse Management Suite 3.5 è possibile registrare i dispositivi utilizzando i campi del record DNS protetto oppure le opzioni di ambito DHCP.

### Informazioni su questa attività


È possibile registrare i dispositivi con il server Wyse Management Suite se i campi del record DNS o le opzioni di ambito DHCP sono impostate mediante i seguenti valori:

- Campi del record DNS SRV:
  - `_WMS_MGMTV2`
  - `_WMS_GROUPTOKENV2`
- Opzioni di ambito DHCP:
  - URL WMS - 201
  - Token di gruppo - 202

### Procedura

1. Accedere ad **Amministrazione portale > Impostazioni console > Individuazione WMS**.
2. Inserire il token di gruppo.
3. Selezionare il tipo di individuazione dall'elenco a discesa **Tipo di individuazione**.
4. Cliccare su **Genera dettagli**.

Vengono visualizzati i dettagli dell'URL WMS crittografato e il token di gruppo.

 **N.B.:** se il certificato Wyse Management Suite viene modificato, il codice DHCP e il DNS protetto devono essere ricreati per registrare un nuovo dispositivo.

## Distribuzione di applicazioni ai thin client

Il criterio di applicazione standard consente di installare un singolo pacchetto di applicazione e richiede il riavvio prima e dopo l'installazione di ciascuna applicazione. Utilizzando il criterio di applicazione avanzato, è possibile installare più pacchetti di applicazione con soli due riavvii. Il criterio di applicazione avanzato inoltre supporta l'esecuzione di script pre e postinstallazione che potrebbero essere necessari per l'installazione di una particolare applicazione. Per ulteriori informazioni, vedere [Appendice B](#).

### Argomenti:

- [Caricamento e distribuzione dell'inventario di immagini firmware ThinOS](#)
- [Creazione e distribuzione del criterio di applicazione standard ai thin client](#)

## Caricamento e distribuzione dell'inventario di immagini firmware ThinOS

Per aggiungere un file all'inventario delle immagini ThinOS, effettuare le seguenti operazioni:

### Procedura

1. Nella scheda **App e dati**, in **Repository di immagini sistema operativo**, fare clic su **ThinOS**.
2. Fare clic su **Aggiungi file firmware**.  
Viene visualizzata la schermata **Aggiungi file**.
3. Per selezionare un file, fare clic su **Sfoggia** e andare al percorso in cui si trova il file.
4. Inserire la descrizione del file.
5. Selezionare la casella di controllo se si desidera sovrascrivere un file esistente.
6. Fare clic su **Carica**.

**N.B.:** il file viene aggiunto al repository quando si seleziona la casella di controllo, ma non viene assegnato a nessuno dei gruppi o dei dispositivi. Per assegnare il file, andare alla relativa pagina di configurazione del dispositivo.

## Creazione e distribuzione del criterio di applicazione standard ai thin client

Per implementare un criterio di applicazione standard ai thin client, effettuare le seguenti operazioni:

1. Nel repository locale, andare a **thinClientApps** e copiare l'applicazione nella cartella.
2. Assicurarsi che l'applicazione sia registrata andando alla scheda **App e dati** e selezionando applicazioni e dati **Thin client** in **Inventario app**.  
**N.B.:** l'interfaccia Inventario app richiede circa due minuti per popolare eventuali programmi aggiunti di recente.
3. In **Criteri app**, fare clic su **Thin client**.
4. Fare clic su **Aggiungi criterio**.
5. Per creare un criterio applicazione, immettere le informazioni appropriate nella finestra **Aggiungi criteri app standard**.
  - a. Selezionare **Nome della policy**, **Gruppo**, **Attività**, **Tipo di dispositivo** e **Applicazione TC**.
  - b. Per implementare questa policy per un determinato sistema operativo o per una piattaforma specifica, selezionare **Filtro sottotipo di sistema operativo** o **Filtro piattaforma**.

Timeout visualizza nel client un messaggio che fornisce all'utente il tempo necessario per salvare il lavoro prima di avviare l'installazione. Specificare il numero di minuti per i quali la finestra di dialogo con messaggio deve essere visualizzata nel client.

- c. Per applicare automaticamente questo criterio a un dispositivo registrato con Wyse Management Suite, selezionare **Applica il criterio a nuovi dispositivi** dall'elenco a discesa **Applica criterio automaticamente**.

**i** **N.B.:**

- Il criterio app viene applicato quando un qualsiasi dispositivo viene spostato nel gruppo definito o registrato direttamente nel gruppo.
- Se si seleziona **Applica il criterio ai dispositivi al momento dell'archiviazione**, il criterio viene applicato automaticamente al dispositivo al momento dell'archiviazione nel server Wyse Management Suite.

6. Per consentire un ritardo nell'esecuzione del criterio, selezionare la casella di controllo **Consenti ritardo dell'esecuzione del criterio**. Se questa opzione è selezionata, vengono abilitati i seguenti menu a discesa:

- Dal menu a discesa **Ore max per ritardo**, selezionare il numero massimo di ore (1-24 ore) di ritardo consentito per l'esecuzione del criterio.
- Dal menu a discesa **Ritardi max**, selezionare il numero di volte (1-3) per le quali è possibile ritardare l'esecuzione del criterio.

7. Per interrompere il processo di installazione dopo aver definito un valore, specificare il numero di minuti nel campo **Timeout installazione applicazione**.

8. Fare clic su **Salva** per creare un criterio.

Viene visualizzato un messaggio per consentire all'amministratore di pianificare questo criterio sui dispositivi in base al gruppo.

9. Selezionare **Sì** per pianificare un processo nella stessa pagina.

Il criterio app/immagine può essere eseguito:

- Immediatamente:** il server esegue il processo immediatamente.
- Nel fuso orario dispositivo:** il server crea un processo per il fuso orario di ciascun dispositivo e pianifica il processo nella data/ora selezionata del fuso orario del dispositivo.
- Nel fuso orario selezionato:** il server crea un processo affinché venga eseguito nella data/ora del fuso orario designato.

10. Per creare il processo, fare clic su **Anteprima** e le pianificazioni vengono visualizzate nella pagina successiva.

11. È possibile controllare lo stato del processo passando alla pagina **Processi**.

# Aggiornamento di Wyse Management Suite dalla versione 2.x alla 3.x

## Prerequisiti

- Accertarsi che vi sia spazio sufficiente sull'unità in cui è installato Wyse Management Suite e che il repository locale sia configurato.
- Se sono stati installati o configurati programmi antivirus o altri strumenti di monitoraggio sulla configurazione di Wyse Management Suite, Dell Technologies consiglia di disabilitare temporaneamente gli strumenti fino al completamento dell'aggiornamento. È inoltre possibile aggiungere l'esclusione appropriata per la directory di installazione, la directory temporanea e la directory del repository locale di Wyse Management Suite.

## Procedura

1. Cliccare due volte sul pacchetto del programma di installazione di Wyse Management Suite 3.x.
2. Nella schermata **Introduzione**, cliccare su **Avanti**.  
Vengono visualizzati i dettagli dell'EULA.
  - i** **N.B.:** Questa schermata viene visualizzata quando si esegue l'aggiornamento da Wyse Management Suite 3.0 a 3.x.
3. Leggere il contratto di licenza.
4. Selezionare la casella di controllo **Accetto i termini del contratto di licenza** e cliccare su **Avanti**.
5. Sulla pagina **Upgrade**, configurare la cartella condivisa e i diritti di accesso per l'utente CIFS. Le opzioni disponibili sono le seguenti:
  - Utilizza utente esistente: selezionare questa opzione per convalidare le credenziali per un utente esistente.
  - Crea nuovo utente: selezionare questa opzione e immettere le credenziali per creare un nuovo utente.
  - i** **N.B.:** Se EM SDK è installato sul server durante l'installazione di Wyse Management Suite precedente, i componenti di Teradici EM SDK vengono aggiornati automaticamente. Se EM SDK non è installato sul dispositivo durante l'installazione precedente, selezionare la casella di controllo Teradici EM SDK per installare e configurare i componenti di Teradici EM SDK.
  - i** **N.B.:** È possibile inoltre installare e aggiornare Teradici EM SDK utilizzando il programma di installazione di Wyse Management Suite.
6. Selezionare la casella di controllo **Associa Memcached a 127.0.0.1** per associare Memcached al server locale 127.0.0.1. Se questa casella di controllo non è selezionata, Memcache è **associato** al FQDN.
7. Selezionare tutte le versioni appropriate di TLS in base ai criteri di supporto dei dispositivi gestiti.
  - i** **N.B.:** La versione di WDA precedente a WDA\_14.4.0.135\_Unified, lo strumento di importazione e l'immagine Merlin a 32 bit non sono compatibili con TLSv1.1 e versioni successive. Selezionare TLSv1.0 se l'ambiente Wyse Management Suite ha dispositivi con versione precedente di WDA, lo strumento di importazione o dispositivi installati con un'immagine Merlin a 32 bit.
8. Cliccare su **Avvia** per aprire la console web di Wyse Management Suite.

# Aggiornamento di Wyse Management Suite dalla versione 3.x alla 3.3

## Prerequisiti

- Accertarsi che vi sia spazio sufficiente sull'unità in cui è installato Wyse Management Suite e che il repository locale sia configurato.
- Se sono stati installati o configurati programmi antivirus o altri strumenti di monitoraggio sulla configurazione di Wyse Management Suite, Dell Technologies consiglia di disabilitare temporaneamente gli strumenti fino al completamento dell'aggiornamento. È inoltre possibile aggiungere l'esclusione appropriata per la directory di installazione, la directory temporanea e la directory del repository locale di Wyse Management Suite.

## Procedura

1. Cliccare due volte sul pacchetto del programma di installazione di Wyse Management Suite 3.2.
2. Nella schermata **Introduzione**, cliccare su **Avanti**.  
Vengono visualizzati i dettagli dell'EULA.
  - i** **N.B.:** Questa schermata viene visualizzata quando si esegue l'aggiornamento da Wyse Management Suite 3.0 a 3.x.
3. Leggere il contratto di licenza.
4. Selezionare la casella di controllo **Accetto i termini del contratto di licenza** e cliccare su **Avanti**.
5. Sulla pagina **Upgrade**, configurare la cartella condivisa e i diritti di accesso per l'utente CIFS. Le opzioni disponibili sono le seguenti:
  - Utilizza utente esistente: selezionare questa opzione per convalidare le credenziali per un utente esistente.
  - Crea nuovo utente: selezionare questa opzione e immettere le credenziali per creare un utente.
  - i** **N.B.:** Se EM SDK è installato sul server durante l'installazione di Wyse Management Suite precedente, i componenti di Teradici EM SDK vengono aggiornati automaticamente. Se EM SDK non è installato sul dispositivo durante l'installazione precedente, selezionare la casella di controllo Teradici EM SDK per installare e configurare i componenti di Teradici EM SDK.
  - i** **N.B.:** È possibile inoltre installare e aggiornare Teradici EM SDK utilizzando il programma di installazione di Wyse Management Suite.
6. Selezionare la casella di controllo **Associa Memcached a 127.0.0.1** per associare Memcached al server locale 127.0.0.1. Se questa casella di controllo non è selezionata, Memcache è **associato** al FQDN.
7. Selezionare una porta per la comunicazione protetta MQTT. La porta predefinita è 8443.
  - i** **N.B.:** Il numero di porta per la comunicazione protetta MQTT non deve essere 0. L'opzione per la selezione della porta viene visualizzata quando si esegue l'aggiornamento di Wyse Management Suite dalla versione 3.1 e 3.1.1 alla versione 3.3.

La finestra **Aggiorna configurazione MQTT** viene visualizzata in assenza di corrispondenza del nome host tra gli URL MQTT nel database.
8. Selezionare la casella di controllo **Applica modifiche consigliate** se si desidera modificare gli URL.
  - i** **N.B.:** La finestra **Aggiorna configurazione MQTT** viene visualizzata quando si esegue l'aggiornamento di Wyse Management Suite dalla versione 3.2 e 3.2.1 alla versione 3.3.
9. Cliccare su **Avanti**.
10. Cliccare su **Avvia** per aprire la console web di Wyse Management Suite.



# Aggiornamento di Wyse Management Suite dalla versione 3.x alla 3.5

## Prerequisiti

- Accertarsi che vi sia spazio sufficiente sull'unità in cui è installato Wyse Management Suite e che il repository locale sia configurato.
- Se sono stati installati o configurati programmi antivirus o altri strumenti di monitoraggio sulla configurazione di Wyse Management Suite, Dell Technologies consiglia di disabilitare temporaneamente gli strumenti fino al completamento dell'aggiornamento. È inoltre possibile aggiungere l'esclusione appropriata per la directory di installazione, la directory temporanea e la directory del repository locale di Wyse Management Suite.

## Procedura

1. Cliccare due volte sul pacchetto di installazione di Wyse Management Suite 3.5.
2. Nella schermata **Introduzione**, cliccare su **Avanti**.  
Vengono visualizzati i dettagli dell'EULA.
  - i** **N.B.:** Questa schermata viene visualizzata quando si esegue l'aggiornamento da Wyse Management Suite 3.0 a 3.x.
3. Leggere il contratto di licenza.
4. Selezionare la casella di controllo **Accetto i termini del contratto di licenza** e cliccare su **Avanti**.
5. Nella pagina **Aggiorna** effettuare le seguenti operazioni:
  - a. Configurare la cartella condivisa e i diritti di accesso per l'utente CIFS. Le opzioni disponibili sono le seguenti:
    - **Utilizza utente esistente:** selezionare questa opzione per convalidare le credenziali per un utente esistente.
    - **Crea nuovo utente:** selezionare questa opzione e inserire le credenziali per creare un nuovo utente.

La password deve contenere più di 8 caratteri.
  - b. Cliccare su **Avanti**.
  - c. Viene visualizzata la schermata **Credenziali account servizio**. Inserendo le credenziali viene creato un utente locale con privilegi minimi. I servizi Dell Wyse Management Suite vengono eseguiti su questo account utente.
  - d. Inserire le credenziali dell'account dei servizi.  
La password deve contenere un minimo di 9 e un massimo di 127 caratteri.
  - e. Cliccare su **Avanti**.  
Viene visualizzata la schermata **Credenziali Software Vault**. Software Vault viene utilizzato per archiviare i dati sensibili richiesti dall'applicazione Dell Wyse Management Suite.
  - f. Inserire la password per Software Vault.  
La password deve contenere più di 8 caratteri.
  - g. Cliccare su **Avanti**.
    - i** **N.B.:** Se EM SDK è installato sul server durante l'installazione di Wyse Management Suite precedente, i componenti di Teradici EM SDK vengono aggiornati automaticamente. Se EM SDK non è stato installato sul dispositivo durante l'installazione precedente, selezionare la casella di controllo **Teradici EM SDK** per installare e configurare i componenti di Teradici EM SDK.
    - i** **N.B.:** È possibile inoltre installare e aggiornare Teradici EM SDK utilizzando il programma di installazione di Wyse Management Suite.
6. Selezionare una porta per la comunicazione protetta MQTT. La porta predefinita è 8443.
  - i** **N.B.:** Il numero di porta per la comunicazione protetta MQTT non deve essere 0. L'opzione per la selezione della porta viene visualizzata quando si esegue l'aggiornamento di Wyse Management Suite dalla versione 3.1 e 3.1.1 alla versione 3.5.
7. Selezionare la casella di controllo **Applica modifiche consigliate** se si desidera modificare gli URL.
  - i** **N.B.:** La finestra **Aggiorna configurazione MQTT** viene visualizzata quando si esegue l'aggiornamento di Wyse Management Suite dalla versione 3.2 e 3.2.1 alla versione 3.5.
8. Cliccare su **Avanti**.

9. Cliccare su **Avvia** per aprire la console web di Wyse Management Suite.

# Aggiornamento di Wyse Management Suite dalla versione 3.x alla 3.6

## Prerequisiti

- Accertarsi che vi sia spazio sufficiente sull'unità in cui è installato Wyse Management Suite e che il repository locale sia configurato.
- Se sono stati installati o configurati programmi antivirus o altri strumenti di monitoraggio sulla configurazione di Wyse Management Suite, Dell Technologies consiglia di disabilitare temporaneamente gli strumenti fino al completamento dell'aggiornamento. È inoltre possibile aggiungere l'esclusione appropriata per la directory di installazione, la directory temporanea e la directory del repository locale di Wyse Management Suite.

## Procedura

1. Cliccare due volte sul pacchetto di installazione di Wyse Management Suite 3.6.

2. Nella schermata **Introduzione**, cliccare su **Avanti**.  
Vengono visualizzati i dettagli dell'EULA.

 **N.B.:** Questa schermata viene visualizzata quando si esegue l'aggiornamento da Wyse Management Suite 3.0 a 3.x.

3. Leggere il contratto di licenza.

4. Selezionare la casella di controllo **Accetto i termini del contratto di licenza** e cliccare su **Avanti**.

5. Nella pagina **Aggiorna** effettuare le seguenti operazioni:

a. Configurare la cartella condivisa e i diritti di accesso per l'utente CIFS. Le opzioni disponibili sono le seguenti:

- **Utilizza utente esistente:** selezionare questa opzione per convalidare le credenziali per un utente esistente.
- **Crea nuovo utente:** selezionare questa opzione e immettere le credenziali per creare un utente.


La password deve contenere più di otto caratteri.

b. Cliccare su **Avanti**.


Viene visualizzata la schermata **Credenziali account servizio**. Selezionare le opzioni in base alla versione esistente di Wyse Management Suite.

• Se si esegue l'aggiornamento da Wyse Management Suite dalla versione 3.3 o 3.3.1 alla 3.6, vengono visualizzate le seguenti opzioni:


- **Crea nuovo utente locale:** selezionare questa opzione per immettere le credenziali e creare un nuovo utente locale con privilegi minimi. Il nuovo utente viene aggiunto al gruppo **Utenti**. Tuttavia, non disporrà dei diritti di amministratore.

 **N.B.:** Il nome utente inserito nella schermata **Credenziali account di servizio** non deve coincidere con il nome utente Teradici. Il nome utente deve contenere da 2 a 20 caratteri. La password deve contenere da 9 a 127 caratteri e almeno un carattere maiuscolo, un carattere minuscolo, un numero e un carattere speciale. Non è consentito l'uso degli spazi per la password.

- **Utilizza un utente locale esistente:** selezionare questa opzione per immettere le credenziali di un utente locale esistente. Viene visualizzato un messaggio quando si seleziona questa opzione. Assicurarsi che l'utente esista già, che disponga dei diritti di accesso al servizio (**SeServiceLogonRight**) e che abbia eseguito correttamente l'accesso al sistema almeno una volta. Dell Technologies consiglia di assicurarsi che l'utente non disponga dei diritti di amministrazione.

 **N.B.:** Se si seleziona questa opzione, la complessità della password non viene verificata e il nome utente immesso deve contenere da 2 a 20 caratteri.

- **Utilizza utente di dominio esistente:** selezionare questa opzione per immettere le credenziali di un utente di dominio esistente. Viene visualizzato un messaggio quando si seleziona questa opzione. Assicurarsi che l'utente esista già nel dominio, che disponga dei diritti di accesso al servizio (**SeServiceLogonRight**) e che abbia eseguito correttamente l'accesso al sistema almeno una volta. Dell Technologies consiglia di assicurarsi che l'utente non disponga dei diritti di amministrazione.

 **N.B.:** Se si seleziona questa opzione, la complessità della password non viene verificata.

- Se si esegue l'aggiornamento da Wyse Management Suite dalla versione 3.5 alla 3.6, immettere le credenziali per creare un utente locale con privilegi minimi. I servizi Dell Wyse Management Suite vengono eseguiti su questo account utente.

c. Cliccare su **Avanti** dopo aver inserito le credenziali.

Viene visualizzata la schermata **Credenziali Software Vault**. Software Vault viene utilizzato per archiviare i dati sensibili richiesti dall'applicazione Dell Wyse Management Suite.

d. Inserire la password per Software Vault.

La password deve contenere più di otto caratteri.

e. Cliccare su **Avanti**.

**i** **N.B.:** Se EM SDK è installato sul server durante l'installazione di Wyse Management Suite precedente, i componenti di Teradici EM SDK vengono aggiornati automaticamente. Se EM SDK non è stato installato sul dispositivo durante l'installazione precedente, selezionare la casella di controllo **Teradici EM SDK** per installare e configurare i componenti di Teradici EM SDK.

**i** **N.B.:** È possibile inoltre installare e aggiornare Teradici EM SDK utilizzando il programma di installazione di Wyse Management Suite.

6. Selezionare una porta per la comunicazione protetta MQTT. La porta predefinita è 8443.

**i** **N.B.:** Il numero di porta per la comunicazione protetta MQTT non deve essere 0. L'opzione per la selezione della porta viene visualizzata quando si esegue l'aggiornamento di Wyse Management Suite dalla versione 3.1 e 3.1.1 alla versione 3.6.

7. Selezionare la casella di controllo **Applica modifiche consigliate** se si desidera modificare gli URL.

**i** **N.B.:** La finestra **Aggiorna configurazione MQTT** viene visualizzata quando si esegue l'aggiornamento di Wyse Management Suite dalla versione 3.2 e 3.2.1 alla versione 3.6.

8. Cliccare su **Avanti**.

9. Cliccare su **Avvia** per aprire la console web di Wyse Management Suite.

# Disinstallazione di Dell Wyse Management Suite

Per disinstallare Wyse Management Suite, effettuare le seguenti operazioni:

1. Fare doppio clic sull'icona **WMS**.

La disinstallazione guidata viene avviata e viene visualizzata la schermata del **programma di disinstallazione di Wyse Management Suite**.

2. Fare clic su **Avanti**. Per impostazione predefinita, è selezionato il pulsante di opzione **Rimuovi** che disinstalla Rimuovere tutti i componenti del programma di installazione Wyse Management Suite.

# Risoluzione dei problemi di Dell Wyse Management Suite

In questa sezione vengono fornite informazioni sulla risoluzione dei problemi per Wyse Management Suite.

## Problemi con l'accesso Wyse Management Suite console web

- Problema: quando si tenta di collegarsi alla console di Wyse Management Suite, la GUI di autenticazione non viene visualizzata e viene visualizzata una pagina Stato HTTP 404.

Soluzione alternativa: interrompere e avviare i servizi nel seguente ordine:

1. Dell WMS: MariaDB
2. Dell WMS: memcached
3. Dell WMS: MongoDB
4. Dell WMS: servizio MQTT broker
5. Dell WMS: Tomcat Service

- Problema: quando si tenta di collegarsi alla console di Wyse Management Suite, la GUI di autenticazione non viene visualizzata, ma viene visualizzato il seguente messaggio di errore:

### Impossibile visualizzare la pagina

Soluzione alternativa: riavviare Dell WMS: Tomcat Service

- Problema: la console Web di Wyse Management Suite non risponde oppure le informazioni nella pagina Web non vengono visualizzate correttamente quando si utilizza Internet Explorer.

Soluzione alternativa:

- Assicurarsi di utilizzare la versione supportata di Internet Explorer.
- Accertarsi che Protezione avanzata di Internet Explorer sia disabilitata.
- Assicurarsi che le impostazioni di visualizzazione compatibilità siano disabilitate.

## Registrazione dei dispositivi con Wyse Management Suite

 **N.B.:** Per informazioni sull'ambiente di sicurezza del cliente, vedere [Wyse Device Agent](#).

- Problema: impossibile registrare i dispositivi con Wyse Management Suite nel cloud pubblico

Soluzione alternativa:


- Accertarsi che le porte 443 e 1883 siano aperte.
- Verificare la connettività di rete e accedere all'applicazione Web Wyse Management dal browser per il cloud pubblico.
- Se l'opzione **Rilevamento automatico** è attivata, verificare se i record DHCP o DNS SVR sono configurati correttamente. Inoltre, controllare l'URL del server e i token di gruppo.
- Controllare se è possibile registrare il dispositivo manualmente.

- Problema: impossibile registrare i dispositivi con Wyse Management Suite nel cloud privato.

Soluzione alternativa:

- Accertarsi che le porte 443 e 1883 siano aperte.
- Verificare la connettività Internet e se è possibile accedere all'applicazione Web Wyse Management dal browser.

- Se è abilitato il rilevamento automatico, verificare se i record DHCP o DNS SRV sono configurati correttamente. Inoltre, controllare l'URL del server e i token di gruppo.
- Controllare se è possibile registrare il dispositivo manualmente.
- Controllare se si utilizzano certificati autofirmati o noti.

 **N.B.:** per impostazione predefinita, Wyse Management Suite installa i certificati autofirmati. La convalida CA deve essere disattivata per consentire ai dispositivi di comunicare con il server Wyse Management Suite.

## Errore durante l'invio dei comandi al dispositivo

Problema: non è possibile inviare comandi quali l'aggiornamento del pacchetto, il riavvio del dispositivo e così via.

Soluzione alternativa:

- Accertarsi che il Dell WMS: MQTT broker sia in esecuzione sul server Wyse Management Suite.
- Controllare se la porta nel 1883 è aperta.
- Accertarsi che il dispositivo non sia arrestato o in stato di sospensione prima di inviare un comando.

## Wyse Device Agent


Il Wyse Device Agent (WDA) è un agente unificato per tutte le soluzioni di gestione thin client. Se si installa WDA, è possibile gestire i thin client tramite Wyse Management Suite.

I seguenti tre tipi di ambienti di sicurezza del cliente sono supportati dal Wyse Device Agent:

- **Ambienti altamente protetti:** per ridurre il rischio posto da Rogue DHCP o server DNS nella discovery di nuovi dispositivi, gli amministratori devono effettuare il login a ciascun dispositivo separatamente e configurare l'URL del server Wyse Management Suite. È possibile utilizzare certificati firmati dall'autorità di certificazione o autofirmati. Tuttavia, Dell consiglia di utilizzare un certificato firmato dall'autorità di certificazione. Nella soluzione di cloud privato Wyse Management Suite con certificato firmato dall'autorità, il certificato deve essere configurato manualmente su ogni dispositivo. Inoltre, il certificato deve essere copiato nella cartella `Configurazione Agent` al fine di preservare il certificato e ridurre il rischio posto da Rogue DHCP o un server DNS anche dopo la ricreazione dell'immagine del dispositivo.

La cartella `Configurazione Agent` è disponibile nella seguente posizione:

- Dispositivi Windows Embedded Standard: `%SYSTEMDRIVE%\Wyse\WCM\ConfigMgmt\Certificates`
- Dispositivi ThinLinux: `/etc/addons.d/WDA/certs`
- Dispositivi ThinOS: `wnos/cacerts/`

 **N.B.:** È necessario importare il certificato in un thin client con sistema operativo ThinOS utilizzando un'unità USB o i percorsi FTP.

- **Ambienti protetti:** per mitigare il rischio posto da Rogue DHCP o server DNS nella discovery di nuovi dispositivi, gli amministratori devono configurare il server Wyse Management Suite utilizzando certificati firmati dall'autorità di certificazione. Il dispositivo può recuperare l'URL del server Wyse Management Suite dai record DHCP/DNS ed eseguire la convalida CA. La soluzione di cloud privato Wyse Management Suite con certificato autofirmato richiede la trasmissione del certificato al dispositivo dopo la prima registrazione, se il dispositivo non dispone del certificato prima della registrazione. Il presente certificato viene conservato anche dopo la ricreazione dell'immagine o il riavvio del dispositivo, per ridurre il rischio posto da Rogue DHCP o server DNS.
- **Ambienti normali:** il dispositivo ottiene l'URL del server Wyse Management Suite dai record DHCP/DNS per il cloud privato Wyse Management Suite, configurato con un certificato firmato dall'autorità o autofirmato. Se l'opzione di convalida CA è disattivata sul dispositivo, l'amministratore di Wyse Management Suite riceve una notifica dopo la prima registrazione del dispositivo. In questo scenario, Dell consiglia agli amministratori di trasmettere un certificato al dispositivo per il quale il server è configurato con un certificato autofirmato. Questo ambiente non è disponibile per il cloud pubblico.



## Risorse aggiuntive

Per esercitazioni video sui seguenti argomenti:

- Per l'installazione Wyse Management Suite, vedere [Installazione di Wyse Management Suite](#).
- Per la configurazione automatica di client ThinOS tramite Wyse Management Suite On-Premise con i tag di opzione DHCP, vedere [Configurazione di dispositivi ThinOS tramite Wyse Management Suite](#).

# Database remoto

Un database remoto o cloud (DB) è un database che è stato progettato per un ambiente virtualizzato, ad esempio cloud ibrido, cloud pubblico o cloud privato. In Wyse Management Suite è possibile configurare il database Mongo (MongoDB) o il database Maria (MariaDB) o entrambi i database in base alle proprie esigenze.

## Argomenti:

- [Configurazione del database Mongo](#)
- [Configurazione del database Maria](#)

## Configurazione del database Mongo

### Prerequisiti

Il database Mongo (MongoDB) opera sul numero di porta TCP (Transmission Control Protocol) 27017.

 **N.B.:** Sostituire eventuali valori in grassetto con le variabili di ambiente, se applicabile.

### Procedura

1. Installare MongoDB versione 4.2.16.
2. Copiare i file MongoDB nel sistema locale - C:\Mongo.
3. Creare le seguenti directory se non sono già presenti:
  - C:\data
  - C:\data\db
  - C:\data\log
4. Andare alla cartella Mongo (C:\Mongo) e creare un file denominato `mongod.cfg`.
5. Aprire il file `mongod.cfg` in un blocco note e aggiungere il seguente script:

```
systemLog:
destination:file
path:c:\data\log\mongod.log
storage:
dbPath:c:\data\db
```

6. Salvare e chiudere il file `mongod.cfg`.
7. Aprire un prompt dei comandi come amministratore ed eseguire il seguente comando:  
`mongod.exe --config "C:\Program Files\MongoDB\Server\4.2\mongod.cfg" -install oppure sc.exe create MongoDB binPath= "\"C:\ProgramFiles\MongoDB\Server\3.2\bin\mongod.exe\" --service --config=\"C:\ProgramFiles\MongoDB\Server\4.2\mongod.cfg\" Displayname= "Dell WMS: MongoDB" start="auto"`  
MongoDB viene installato.
8. Per avviare i servizi MongoDB, eseguire il seguente comando:  
`net start mongoDB`
9. Per avviare il database Mongo, eseguire il seguente comando:  
`mongo.exe`
10. Per aprire il database amministratore predefinito, eseguire il seguente comando:  
`use admin;`
11. Dopo che è stato visualizzato il foglio MongoDB, eseguire i seguenti comandi:

```
db.createUser (
{
```

```
user:"wmsuser",
pwd:"PASSWORD",
roles:[{role:"userAdminAnyDatabase",db:"admin"},
{role:"dbAdminAnyDatabase",db:"admin"},
{role:"readWriteAnyDatabase",db:"admin"},
{role:"dbOwner",db:"stratus"}]
}
)
```

12. Per passare al database Stratus, eseguire il seguente comando:

```
use stratus;
```

13. Per interrompere i servizi MongoDB, eseguire il seguente comando:

```
net stop mongoDB
```

14. Aggiungere un'autorizzazione di autenticazione al DB. amministratore. Modificare il file `mongod.cfg` come indicato di seguito:

```
systemLog:
destination:file
path:c:\data\log\mongod.log
storage:
dbPath:c:\data\db
security:
authorization:enabled
```

15. Per riavviare il servizio MongoDB, eseguire quanto segue:

```
net Start mongoDB;
```

### Fasi successive

Nel programma di installazione di Wyse Management Suite, l'amministratore deve utilizzare lo stesso nome utente e la stessa password che è stata creata per accedere ai database Stratus in MongoDB. Per informazioni sull'impostazione di MongoDB nel programma di installazione di Wyse Management Suite, consultare [Installazione personalizzata](#).

## Configurazione del database Maria

Il database Maria (MariaDB) opera sul numero di porta TCP (Transmission Control Protocol) 3306.

### Informazioni su questa attività



#### N.B.:


- L'indirizzo IP visualizzato qui appartiene al server Wyse Management Suite che ospita i componenti Web.
- Sostituire eventuali valori in grassetto con le variabili di ambiente, se applicabile.

Per configurare MariaDB, effettuare le seguenti operazioni:

### Procedura

1. Installare MariaDB versione 10.2.29.
2. Andare al percorso di installazione di MariaDB - `C:\Program Files\MariaDB 10.2\bin>mysql.exe -u root -p`.
3. Fornire la password radice creata durante l'installazione
4. Creare il database Stratus - `DEFAULT CHARACTER SET utf8 DEFAULT COLLATE utf8_unicode_ci;`
5. Creare l'utente `'stratus'@'localhost';`
6. Creare l'utente `'stratus'@'IP ADDRESS';`
7. Impostare una password per `'stratus'@'localhost'=password('PASSWORD');`
8. Impostare una password per `'stratus'@'IP ADDRESS'=password('PASSWORD');`
9. Fornire tutti i privilegi su `*.* to 'stratus'@'IP ADDRESS'` identificato da `'PASSWORD'` con un'opzione di concessione.
10. Fornire tutti i privilegi su `*.* to 'stratus'@'localhost'` identificato da `'PASSWORD'` con un'opzione di concessione.

### Fasi successive

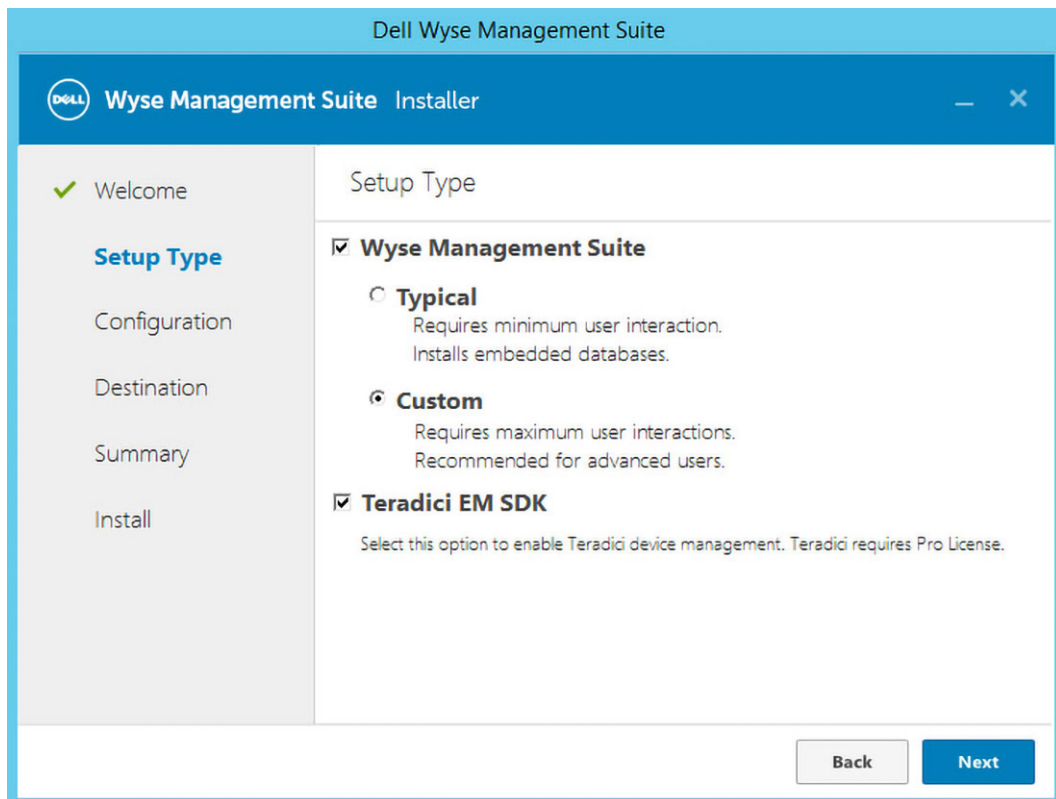
 **N.B.:** per configurare la porta personalizzata per MariaDB, andare a `C:\Program Files\MariaDB 10.2\bin>mysql.exe -u root -p -P<custom port>` nel secondo passaggio.

Nel programma di installazione di Wyse Management Suite, l'amministratore deve utilizzare lo stesso nome utente e la stessa password creati per accedere ai database Stratus in MariaDB. Per informazioni sull'impostazione di MariaDB nel programma di installazione di Wyse Management Suite, consultare [Installazione personalizzata](#).

# Installazione personalizzata

Nell'installazione personalizzata, è possibile selezionare un database per configurare Wyse Management Suite ed è necessario conoscere il funzionamento tecnico di base di Wyse Management Suite. Dell consiglia l'installazione personalizzata solo per gli utenti avanzati.

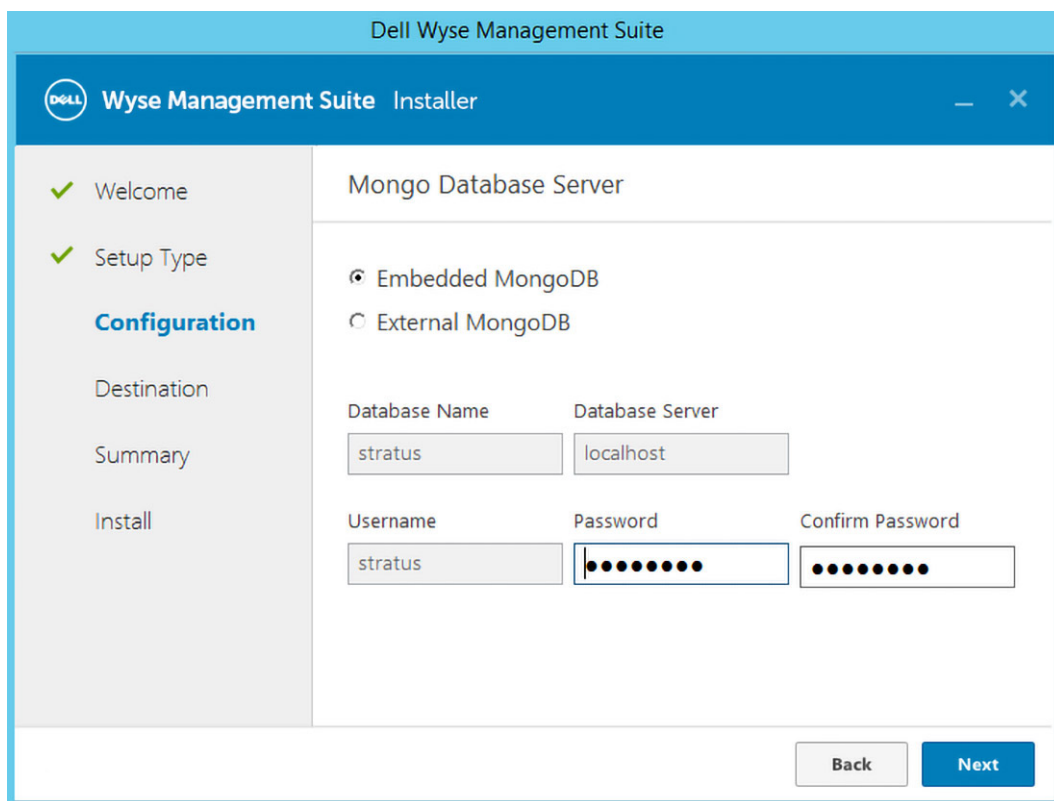
1. Selezionare **Tipo di configurazione Personalizzata** e cliccare su **Avanti**.



**Figura 12. Tipo di configurazione**

Viene visualizzata la pagina **Server database Mongo**.

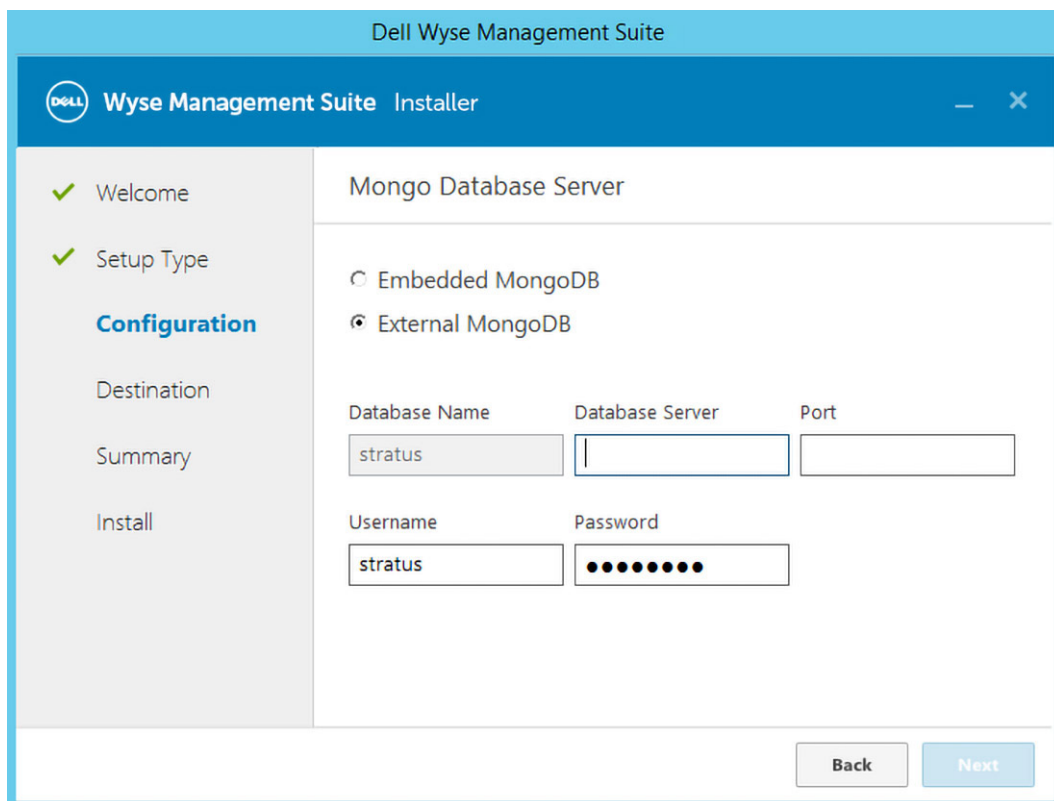
2. Selezionare **MongoDB integrato** o **MongoDB esterno** come server di database Mongo.
  - Se si seleziona **MongoDB integrato**, fornire la propria password e cliccare su **Successivo**
    - ① **N.B.:** La password deve contenere un minimo di 9 e un massimo di 31 caratteri.
    - ① **N.B.:** i dettagli relativi al nome utente e al server di database non sono richiesti se viene selezionato il database Mongo integrato e i rispettivi campi vengono visualizzati in grigio.



**Figura 13. Server di database Mongo integrato**

- Se si seleziona **MongoDB esterno**, fornire nome utente, password, dettagli del server di database e dettagli relativi alle porte e cliccare su **Avanti**.

**i** **N.B.:** Il campo della porta popola la porta predefinita che può essere modificata.



**Figura 14. MongoDB esterno**

Viene visualizzata la pagina **server di database MariaDB**.

3. Selezionare **MariaDB integrato** o **MariaDB esterno** come server di database MariaDB.
  - Se si seleziona **MariaDB integrato**, fornire nome utente e la password e cliccare su **Avanti**.



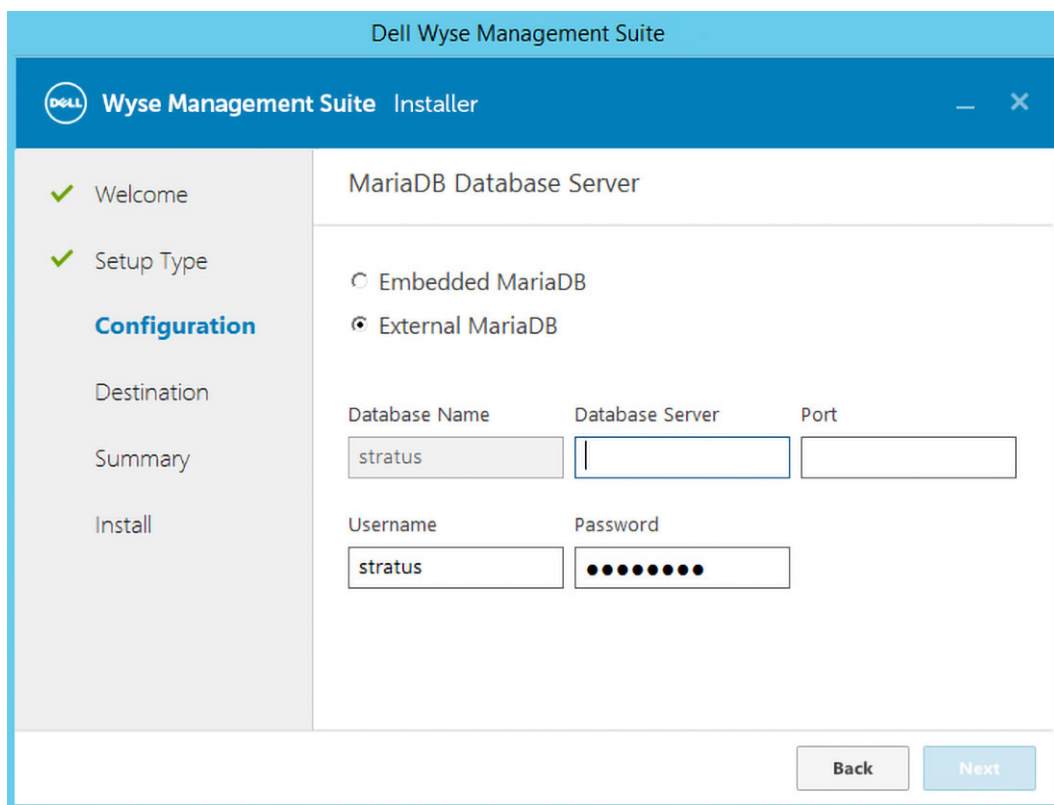
**N.B.:** La password deve contenere un minimo di 9 e un massimo di 31 caratteri.

The screenshot shows the 'MariaDB Database Server' configuration window in the Dell Wyse Management Suite Installer. The window title is 'Dell Wyse Management Suite' and the subtitle is 'Wyse Management Suite Installer'. On the left, a navigation pane shows the progress: 'Welcome' and 'Setup Type' are completed with green checkmarks, 'Configuration' is the current step, and 'Destination', 'Summary', and 'Install' are yet to be completed. The main area is titled 'MariaDB Database Server' and contains two radio button options: 'Embedded MariaDB' (selected) and 'External MariaDB'. Below these are input fields for 'Database Name' (containing 'stratus') and 'Database Server' (containing 'localhost'). Further down are fields for 'Username' (containing 'stratus'), 'Password' (masked with 10 dots), and 'Confirm Password' (masked with 10 dots). At the bottom right, there are 'Back' and 'Next' buttons.

**Figura 15. MariaDB integrato**

- Se si seleziona **MariaDB esterno**, fornire nome utente, password, dettagli del server di database e dettagli relativi alle porte, quindi cliccare **Avanti**.

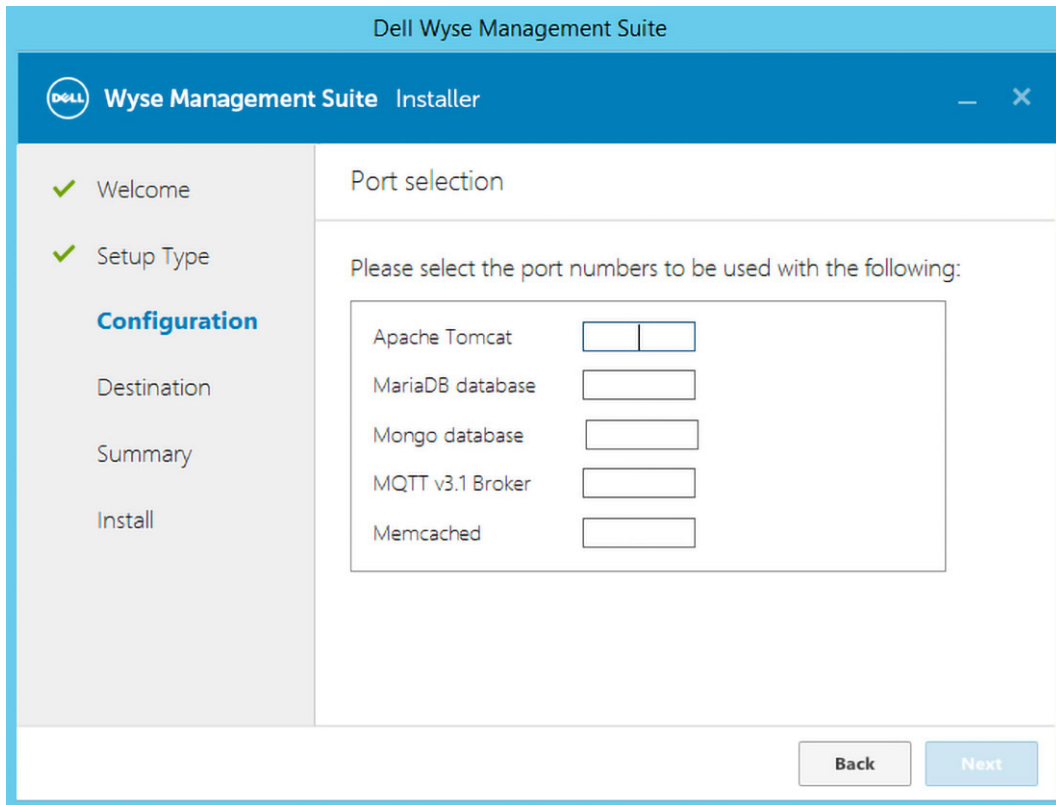
Il campo della porta popola la porta predefinita che può essere modificata.



**Figura 16. MariaDB esterno**

4. Viene visualizzata la pagina **Porta** che consente di personalizzare le porte per i seguenti database:
- Apache Tomcat
  - Database MySQL
  - Database Mongo
  - Gestore MQTT v3.1
  - Memcached





**Figura 17. Selezione della porta**

**i N.B.:** Wyse Management Suite utilizza il database Maria e il database Mongo per le seguenti operazioni:

Database Maria: database relazionale per i dati che richiedono struttura ben definita e normalizzazione

Database Mongo: database non SQL per prestazioni e scalabilità

Per completare l'installazione, seguire la procedura descritta nella sezione [Installazione on-premise di WMS e configurazione iniziale](#).

# Accedere al repository di file di Wyse Management Suite

I **repository di file** sono luoghi in cui i **file** vengono memorizzati e organizzati. Wyse Management Suite dispone di due tipi di repository:

- **Repository locale:** durante l'installazione del private cloud di Wyse Management Suite, fornire il percorso del repository locale nel programma di installazione di Wyse Management Suite. Dopo l'installazione, andare ad **Amministratore portale > Repository di file** e selezionare il repository locale. Cliccare sull'opzione **Modifica** per visualizzare e modificare le impostazioni del repository.
- **Wyse Management Suite repository:** accedere al public cloud di Wyse Management Suite, andare ad **Amministratore portale > Repository di file** e scaricare il programma di installazione di Wyse Management Suite Repository. Dopo l'installazione, registrare Wyse Management Suite Repository nel server di gestione di Wyse Management Suite fornendo le informazioni richieste.

È possibile abilitare l'opzione **Replica automatica** per effettuare la replica dei file aggiunti da uno qualsiasi dei repository di file ad altri repository. Quando si abilita questa opzione, viene visualizzato un messaggio di avviso. È possibile selezionare la casella di controllo **Replica file esistenti** per replicare i file esistenti nei propri repository di file.

L'opzione **Replica file esistenti** è valida se il repository è già registrato. Quando un nuovo repository viene registrato, tutti i file vengono copiati nel nuovo repository. È possibile visualizzare lo stato di replica dei file nella pagina **Eventi**.

I modelli `Image Pull` non vengono replicati automaticamente in altri repository. È necessario copiare questi file manualmente.

La funzione di replica file è supportata solo su repository di Wyse Management Suite 2.0 e versioni successive.

Non è possibile importare un certificato autofirmato del repository remoto nel server Wyse Management Suite. Se la convalida CA è abilitata per il repository remoto, la replica dei file dal repository remoto al repository locale non riesce.

La versione TLS selezionata deve essere uguale o successiva alla versione TLS configurata nel server Wyse Management Suite. Accertarsi di selezionare tutte le versioni appropriate di TLS in base ai criteri di supporto dei dispositivi gestiti.

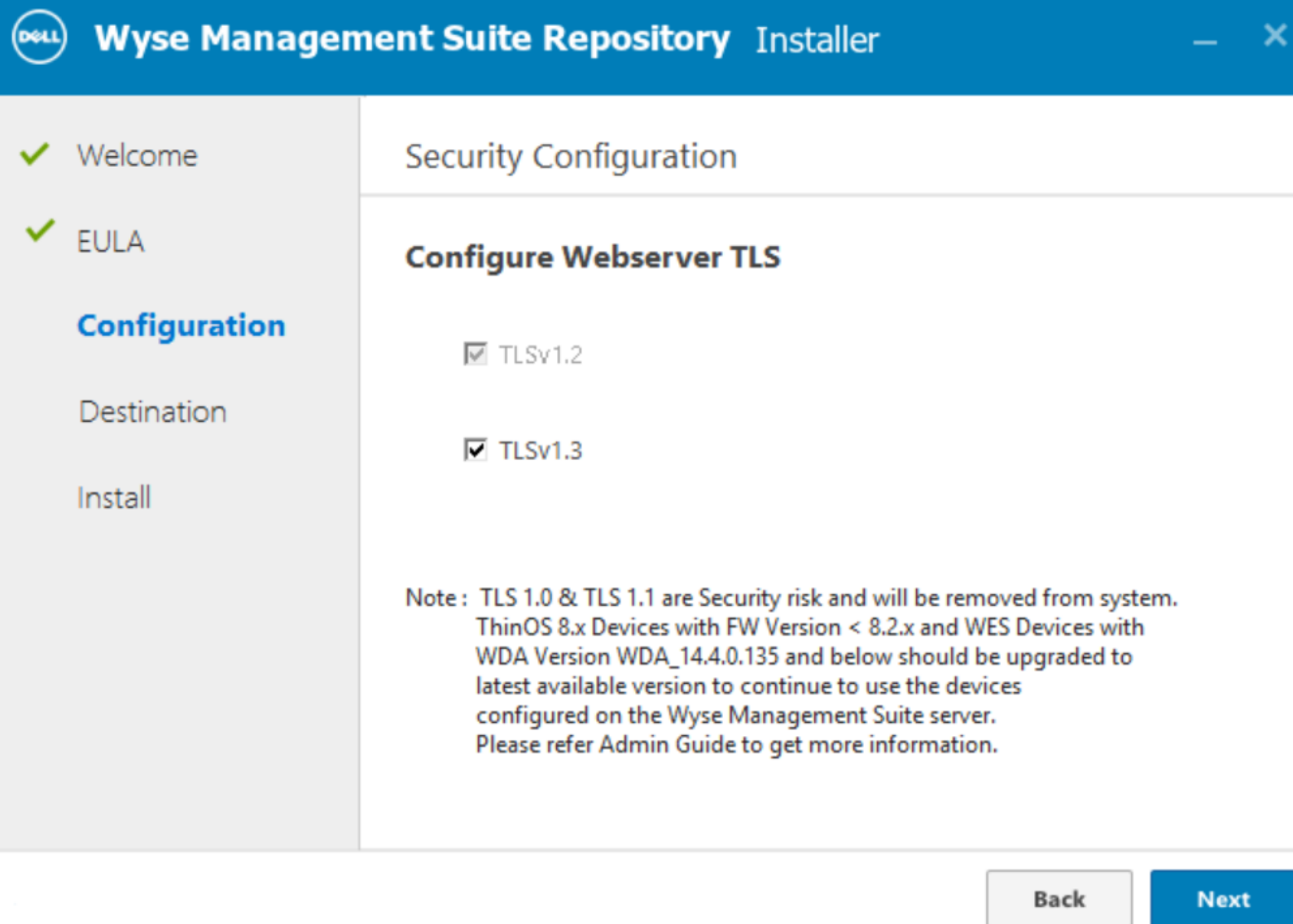


Figura 18. Programma di installazione di Wyse Management Suite Repository

**N.B.:** Non selezionare TLSv 1.1 e versioni successive se la versione di WDA nel dispositivo Windows Embedded è inferiore a 14.4.0.153\_Unified e se si utilizza l'agente di imaging Merlin. TLSv 1.1 e versioni successive non devono essere selezionate se si utilizza lo strumento di importazione per eseguire la migrazione da Wyse Device Manager a Wyse Management Suite.

Per utilizzare Wyse Management Suite Repository, procedere come segue:

1. Scaricare Wyse Management Suite Repository dalla console del public cloud.
2. Dopo il processo di installazione, avviare l'applicazione.
3. Nella pagina Wyse Management Suite Repository, immettere le credenziali per registrare Wyse Management Suite Repository nel server Wyse Management Suite.
4. Se si abilita l'opzione **Registra sul portale di gestione WMS pubblico**, è possibile registrare il repository nel public cloud di Wyse Management Suite.
5. Cliccare sull'opzione **Sincronizza file** per inviare il comando di sincronizzazione file.
6. Cliccare su **Archivia**, quindi cliccare su **Invia comando** per inviare il comando informazioni dispositivo al dispositivo.
7. Cliccare sull'opzione **Annulla registrazione** per annullare la registrazione del servizio on-premise.
8. Cliccare su **Modifica** per modificare i file.

9. Dall'elenco a discesa dell'opzione **Download simultanei di file:**, selezionare il numero di file.
10. Abilitare o disabilitare l'opzione **Wake on LAN**.
11. Abilitare o disabilitare l'opzione **Upload e download di file rapido (HTTP)**.
  - Quando HTTP è abilitato, l'upload e il download dei file avvengono tramite HTTP.
  - Quando HTTP non è abilitato, l'upload e il download dei file avvengono tramite HTTPS.
12. Selezionare la casella di controllo **Convalida certificato** per attivare la Convalida CA per il public cloud.
  - i** **N.B.:** Quando Convalida CA dal server Wyse Management Suite è attivata, il certificato dovrebbe essere presente nel client. Tutte le operazioni, ad esempio App e dati, pull o push dell'immagine, vengono eseguite correttamente. Se il certificato non è presente nel client, il server Wyse Management Suite visualizza il messaggio di controllo generico **Impossibile convalidare autorità di certificazione** nella pagina **Eventi**. Tutte le operazioni, ad esempio App e dati, pull o push dell'immagine, non vengono eseguite correttamente. Inoltre, quando la Convalida CA dal server Wyse Management Suite è disabilitata, la comunicazione tra server e client avviene in un canale sicuro senza convalida Firma certificato.
13. Aggiungere una nota nella casella fornita.
14. Cliccare su **Salva impostazioni**.

# Creazione e configurazione dei tag di opzione DHCP

## Informazioni su questa attività

**N.B.:** Per informazioni sull'ambiente di sicurezza del cliente, vedere [Wyse Device Agent](#).

Per creare un'opzione DHCP, procedere come segue:

## Procedura

1. Aprire Server Manager.
2. Andare a **Strumenti** e fare clic su **Opzione DHCP**.
3. Andare a **FQDN** > **IPv4** e fare clic con il pulsante destro del mouse su **IPv4**.

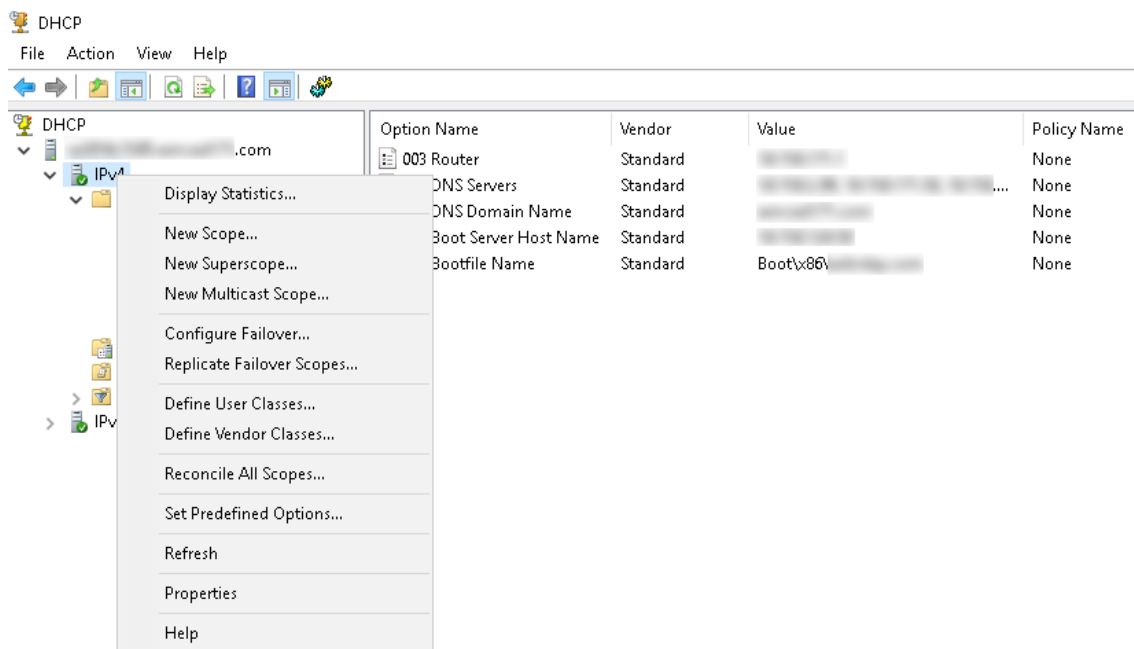


Figura 19. DHCP

4. Fare clic su **Imposta opzioni predefinite**.  
Viene visualizzata la finestra **Opzioni e valori predefiniti**.
5. Dall'elenco a discesa **Classe di opzioni**, selezionare il valore **Opzione standard DHCP**.

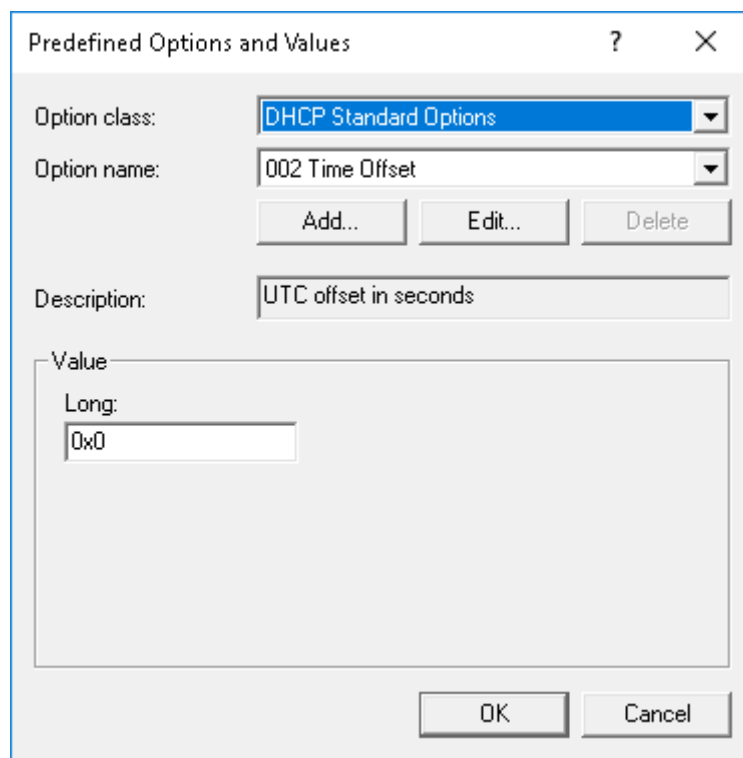


Figura 20. Opzioni e valori predefiniti

6. Fare clic su **Aggiungi**.  
Viene visualizzata la finestra **Tipo di opzione**.

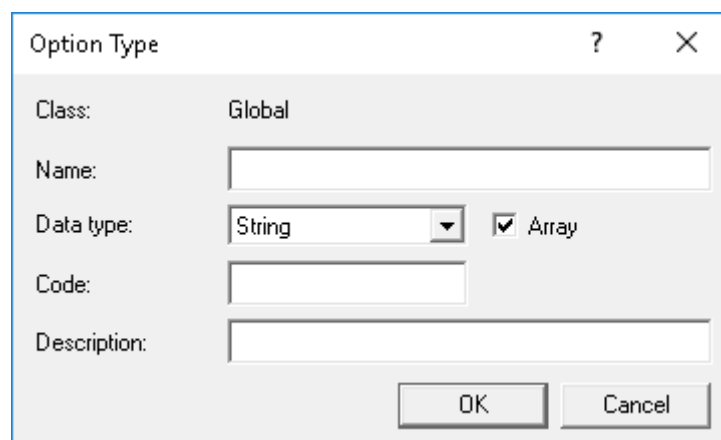


Figura 21. Tipo di opzione

### Esempio

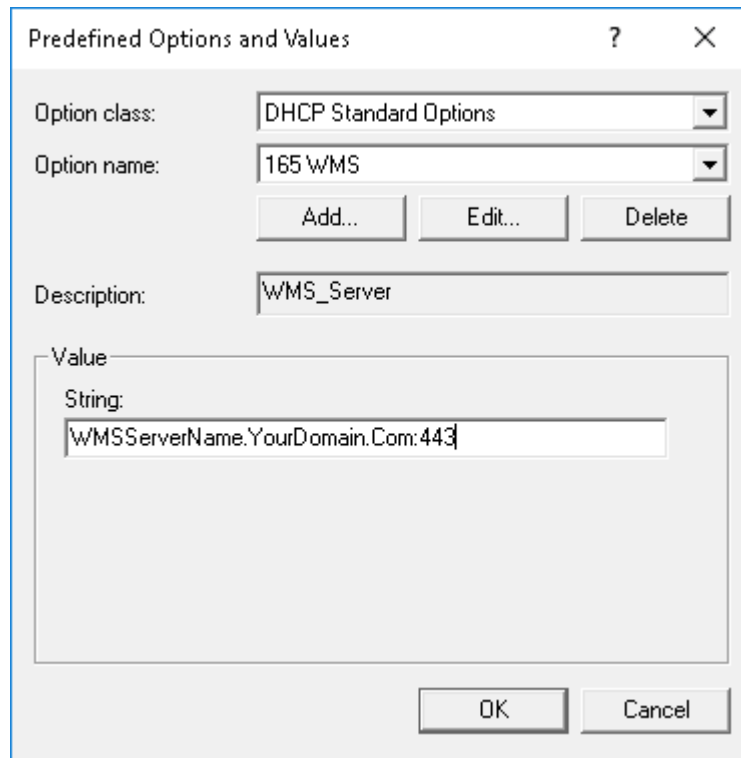
Le opzioni devono essere aggiunte alle opzioni server del server DHCP oppure alle opzioni di ambito dell'ambito DHCP.

### Configurazione dei tag di opzione DHCP

- Per creare il tag opzione dell'URL del server Wyse Management Suite 165, procedere come segue:
  1. Immettere i valori seguenti e fare clic su **OK**.
    - Nome: WMS
    - Tipo di dati: stringa
    - Codice: 165
    - Descrizione: WMS\_Server
  2. Immettere il seguente valore e fare clic su **OK**.

Stringa: WMS FQDN

Ad esempio, WMSServerName.YourDomain.Com:443



The image shows a dialog box titled "Predefined Options and Values". It has a standard Windows-style title bar with a question mark and a close button. The dialog contains several fields and buttons:

- Option class:** A dropdown menu showing "DHCP Standard Options".
- Option name:** A dropdown menu showing "165 WMS".
- Buttons:** Three buttons labeled "Add...", "Edit...", and "Delete" are positioned below the "Option name" field.
- Description:** A text input field containing "WMS\_Server".
- Value:** A section titled "Value" containing a "String:" label and a text input field with the value "WMSServerName.YourDomain.Com:443".
- Bottom Buttons:** Two buttons labeled "OK" and "Cancel" are at the bottom right of the dialog.

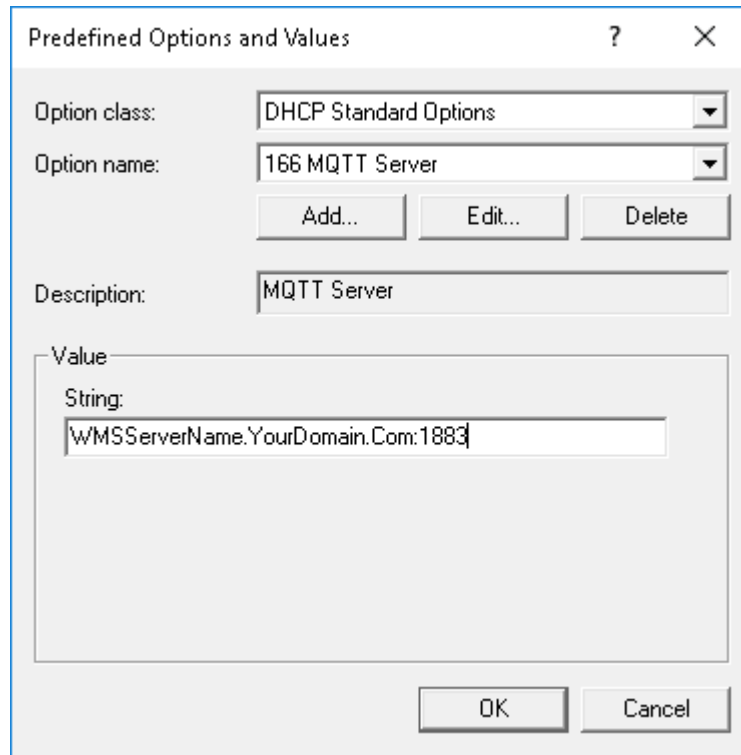
**Figura 22. Tag opzione URL del server Wyse Management Suite 165**

- Per creare il tag opzione dell'URL del server MQTT 166, procedere come segue:

1. Immettere i valori seguenti e fare clic su **OK**.
  - Nome: MQTT
  - Tipo di dati: stringa
  - Codice: 166
  - Descrizione: server MQTT
2. Immettere il seguente valore e fare clic su **OK**.

Stringa: MQTT FQDN

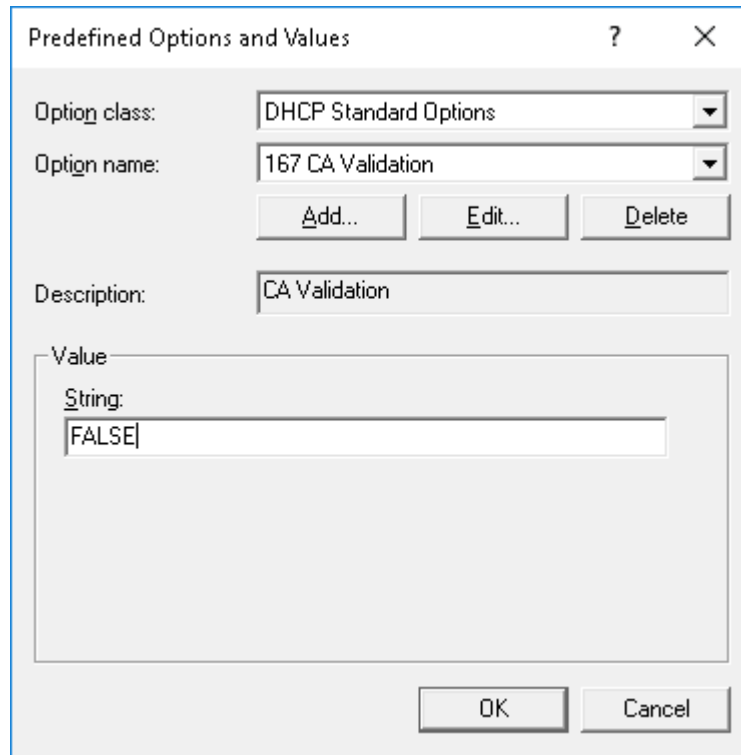
Ad esempio, WMSServerName.YourDomain.Com:1883



**Figura 23. Tag opzione URL del server Wyse Management Suite 166**

- Per creare il tag opzione dell'URL del server di convalida CA Wyse Management Suite 167:
  1. Immettere i valori seguenti e fare clic su **OK**.
    - Nome: convalida CA
    - Tipo di dati: stringa
    - Codice: 167
    - Descrizione: convalida CA
  2. Immettere i valori seguenti e fare clic su **OK**.
    - String: TRUE/FALSE





**Figura 24. Tag opzione URL del server Wyse Management Suite 167**

- Per creare il tag opzione dell'URL del server del token di gruppo Wyse Management 199, procedere come segue:
  1. Immettere i valori seguenti e fare clic su **OK**.
    - Nome: token di gruppo
    - Tipo di dati: stringa
    - Codice: 199
    - Descrizione: token di gruppo
  2. Immettere i valori seguenti e fare clic su **OK**.
    - Stringa: defa-quarantine

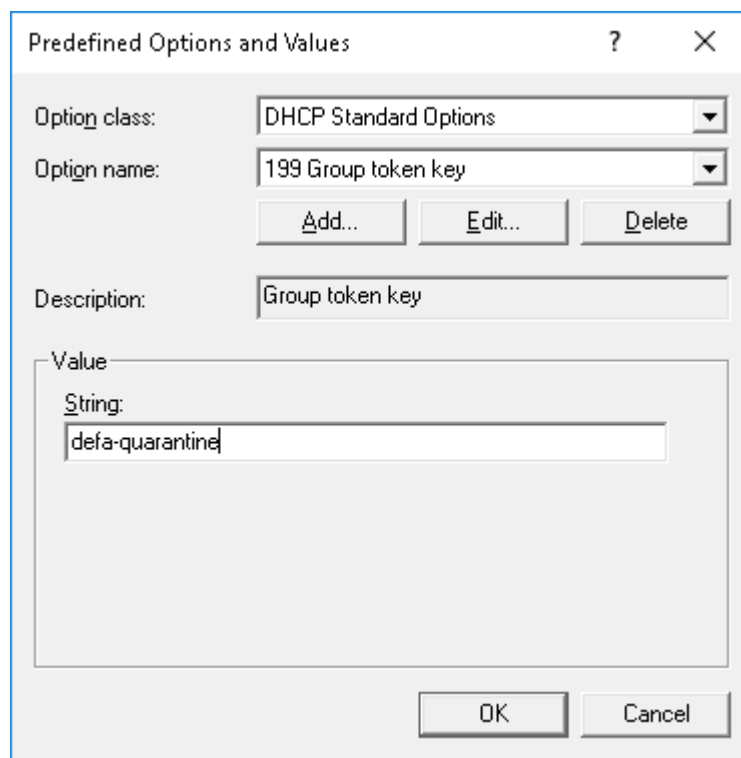


Figura 25. Tag opzione URL del server Wyse Management Suite 199

# Creazione e configurazione dei record DNS SRV

## Informazioni su questa attività

**N.B.:** Per informazioni sull'ambiente di sicurezza del cliente, vedere [Wyse Device Agent](#).

Per creare un record SRV DNS, procedere come segue:

## Procedura

1. Aprire Server Manager.
2. Andare a **Strumenti** e fare clic su **Opzione DNS**.
3. Andare a **DNS Nome host server DNS Zone di ricerca diretta** > **Dominio \_tcp** e fare clic con il pulsante destro del mouse su **\_tcp option**.

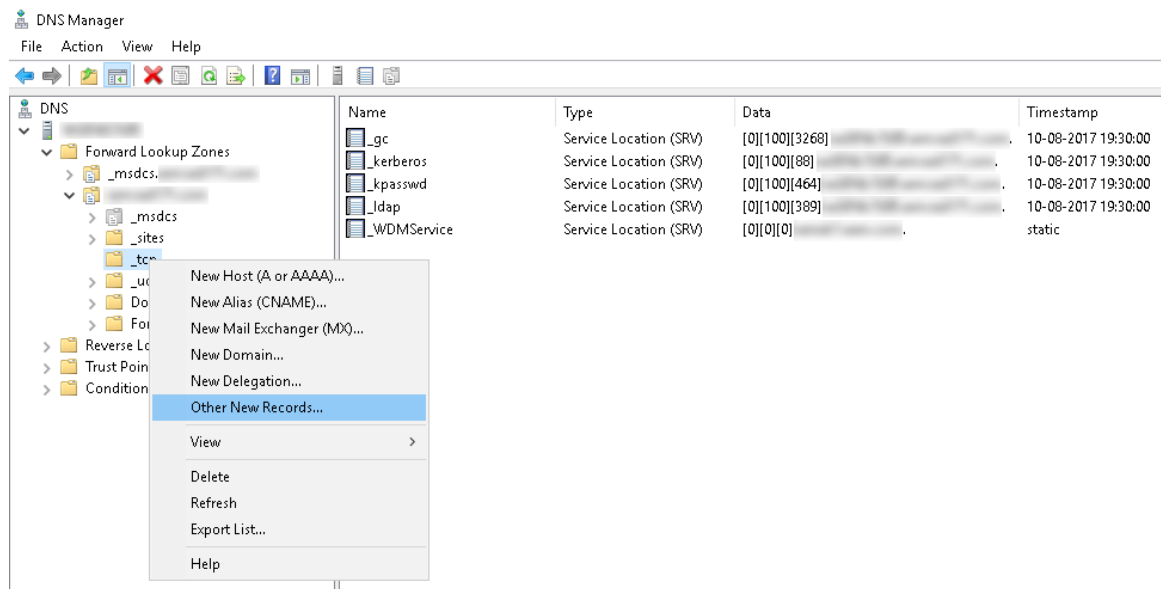
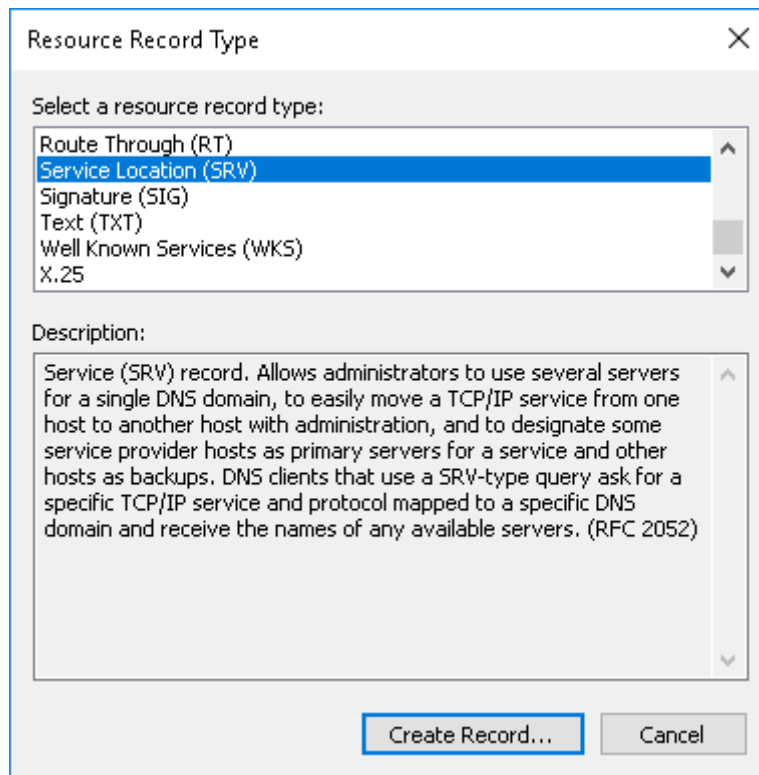


Figura 26. DNS manager

4. Fare clic su **Altri record nuovi**.  
Viene visualizzata la finestra **Tipo di record risorsa**.
5. Selezionare **Posizione servizio (SRV)**, fare clic su **Crea record** ed effettuare le seguenti operazioni:



**Figura 27. Tipo di record risorsa**

- a. Per creare il nuovo record server Wyse Management Suite, immettere i seguenti dettagli e fare clic su **OK**.
- Servizio — `_WMS_MGMT`
  - Protocollo — `_tcp`
  - Numero di porta - 443
  - Host che offre questo servizio - FQDN del server WMS

New Resource Record

Service Location (SRV)

Domain: [redacted]

Service: \_WMS\_MGMT

Protocol: \_tcp

Priority: 0

Weight: 0

Port number: 443

Host offering this service:  
FQDN of WMS server

Allow any authenticated user to update all DNS records with the same name. This setting applies only to DNS records for a new name.

OK Cancel Help

Figura 28. Servizio \_WMS\_MGMT

- b. Per creare il record server MQTT, immettere i valori seguenti, quindi fare clic su **OK**.
- Servizio - \_WMS\_MQTT
  - Protocollo — \_tcp
  - Numero di porta - 1883
  - Host che offre questo servizio - FQDN del server MQTT

New Resource Record

Service Location (SRV)

Domain: .

Service: \_WMS\_MQTT

Protocol: \_tcp

Priority: 0

Weight: 0

Port number: 1883

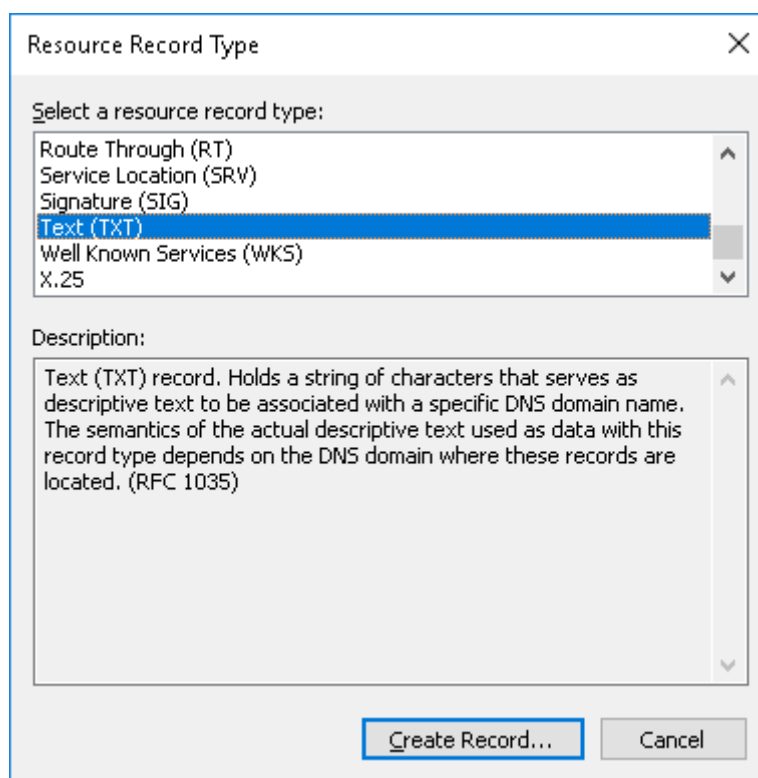
Host offering this service:  
FQDN of MQTT server

Allow any authenticated user to update all DNS records with the same name. This setting applies only to DNS records for a new name.

OK Cancel Help

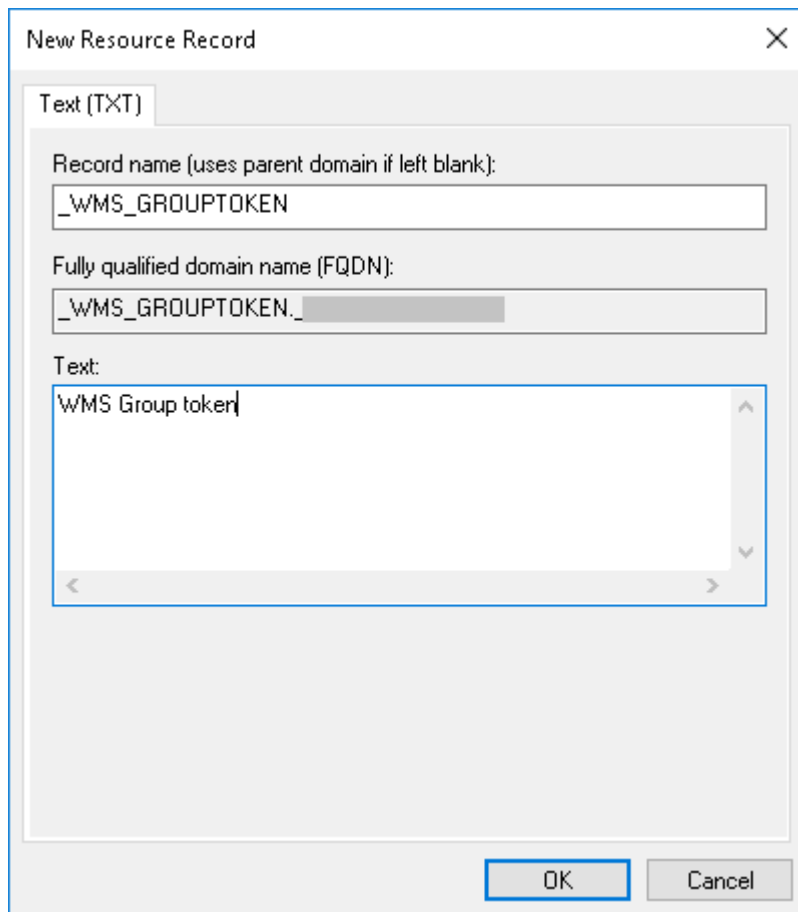
Figura 29. Servizio \_WMS\_MQTT

6. Andare a **DNS Nome host server DNS Zone di ricerca diretta** > **Dominio** e fare clic sul dominio con il pulsante destro del mouse.
7. Fare clic su **Altri record nuovi**.
8. Selezionare **Testo (TXT)**, fare clic su **Crea record** ed effettuare le seguenti operazioni:



**Figura 30. Tipo di record risorsa**

- a. Per creare il record Token di gruppo di Wyse Management Suite, immettere i valori seguenti e fare clic su **OK**.
- Nome record - `_WMS_GROUPTOKEN`
  - Testo - Token di gruppo WMS



**Figura 31. Nome record \_WMS\_GROUPTOKEN**

- b. Per creare il record di convalida CA di Wyse Management Suite, immettere i valori seguenti, quindi fare clic su **OK**.
- Nome record - \_WMS\_CAVALIDATION
  - Testo — TRUE/FALSE



New Resource Record

Text (TXT)

Record name (uses parent domain if left blank):  
\_WMS\_CAVALIDATION

Fully qualified domain name (FQDN):  
\_WMS\_CAVALIDATION.

Text:  
False

OK Cancel



Figura 32. Nome record `_WMS_CAVALIDATION`

# Creazione e distribuzione del criterio di applicazione standard ai thin client

## Informazioni su questa attività

Per implementare un criterio di applicazione standard ai thin client, effettuare le seguenti operazioni:

## Procedura

1. Nel repository locale, andare a **thinClientApps** e copiare l'applicazione nella cartella.
2. Assicurarsi che l'applicazione sia registrata andando alla scheda **App e dati** e selezionando applicazioni e dati **Thin Client** in **Inventario app**.
  -  **N.B.:** l'interfaccia Inventario app richiede circa due minuti per popolare eventuali programmi aggiunti di recente.
3. In **Criteri app**, cliccare su **Thin client**.
4. Cliccare su **Aggiungi criterio**.
5. Per creare un criterio applicazione, immettere le informazioni appropriate nella finestra **Aggiungi criteri app standard**.
  - Selezionare **Nome della policy**, **Gruppo**, **Attività**, **Tipo di dispositivo** e **Applicazione TC**.
  - Per implementare questa policy per un determinato sistema operativo o per una piattaforma specifica, selezionare **Filtro sottotipo di sistema operativo**, **Filtro piattaforma** o **Filtro produttore**. Timeout visualizza nel client un messaggio che fornisce all'utente il tempo necessario per salvare il lavoro prima di avviare l'installazione. Specificare il numero di minuti per i quali la finestra di dialogo con messaggio deve essere visualizzata nel client.
  - Per applicare automaticamente questo criterio a un dispositivo registrato con Wyse Management Suite, selezionare **Applica il criterio a nuovi dispositivi** dall'elenco a discesa **Applica criterio automaticamente**.
  -  **N.B.:** Il criterio app viene applicato quando un qualsiasi dispositivo viene spostato nel gruppo definito o registrato direttamente nel gruppo. Se si seleziona **Applica il criterio ai dispositivi al momento dell'archiviazione**, il criterio viene applicato automaticamente al dispositivo al momento dell'archiviazione nel server Wyse Management Suite.
6. Per consentire un ritardo nell'esecuzione del criterio, selezionare la casella di controllo **Consenti ritardo dell'esecuzione del criterio**. Se questa opzione è selezionata, vengono abilitati i seguenti menu a discesa:
  - Dal menu a discesa **Ore max per ritardo**, selezionare il numero massimo di ore (1-24 ore) di ritardo consentito per l'esecuzione del criterio.
  - Dal menu a discesa **Ritardi max**, selezionare il numero di volte (1- 3) per le quali è possibile ritardare l'esecuzione del criterio.
7. Per interrompere il processo di installazione dopo aver definito un valore, specificare il numero di minuti nel campo **Timeout installazione applicazione**.
8. Cliccare su **Salva** per creare un criterio.  
Viene visualizzato un messaggio per consentire all'amministratore di pianificare questo criterio sui dispositivi in base al gruppo.
9. Selezionare **Sì** per pianificare un processo nella stessa pagina. Il criterio app/immagine può essere eseguito:
  - **Immediatamente:** il server esegue il processo immediatamente.
  - **Nel fuso orario dispositivo:** il server crea un processo per il fuso orario di ciascun dispositivo e pianifica il processo nella data/ora selezionata del fuso orario del dispositivo.
  - **Nel fuso orario selezionato:** il server crea un processo affinché venga eseguito nella data/ora del fuso orario designato.
10. Per creare il processo, cliccare su **Anteprima** e le pianificazioni vengono visualizzate nella pagina successiva.
11. È possibile controllare lo stato del processo passando alla pagina **Processi**.

# Registrazione manuale di Dell Hybrid Client

## Prerequisiti

Prima di registrare il dispositivo, accertarsi che il dispositivo sia connesso alla rete al fine di contattare il server Wyse Management Suite.

**i** **N.B.:** È possibile registrare o annullare la registrazione del dispositivo solo dall'account utente guest.

## Procedura

1. Accedere al client ibrido come utente guest.
2. Nella barra superiore, cliccare sull'icona **Dell Client Agent**.

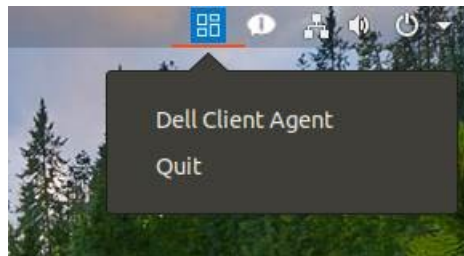


Figura 33. Icona DCA

3. Cliccare su **Dell Client Agent**.  
Viene visualizzata la finestra di dialogo **Dell Client Agent**.
4. Cliccare su **Registrazione**.  
Lo stato predefinito viene visualizzato come **Rilevamento in corso**.
5. Per registrarsi manualmente, cliccare sul pulsante **Annulla**.
6. Nel campo **Server WMS**, inserire l'URL del server Wyse Management Suite.
7. Nel campo **Token di gruppo**, inserire il codice di registrazione del gruppo. Il token di gruppo è una chiave univoca per registrare i dispositivi direttamente con i gruppi.  
**i** **N.B.:** Se i campi del tenant e del gruppo sono vuoti, il dispositivo viene registrato con il gruppo non gestito. Tuttavia, il token di gruppo è obbligatorio per registrare il dispositivo con un public cloud.
8. Cliccare sul pulsante **ON/OFF** per abilitare o disabilitare l'opzione **Convalida autorità certificazione server**. Abilitare questa opzione per eseguire la convalida del certificato server per tutte le comunicazioni tra il dispositivo e il server.  
L'opzione Convalida CA è abilitata automaticamente e non può essere disabilitata se viene inserito un URL del public cloud.
9. Cliccare su **Registra** per registrare il client ibrido sul server Wyse Management Suite.  
Quando il client ibrido viene registrato correttamente, lo stato viene visualizzato come **Registrato** con il segno di spunta verde accanto all'etichetta **Stato della registrazione**. La didascalia del pulsante **Registra** cambia in **Annulla registrazione**.

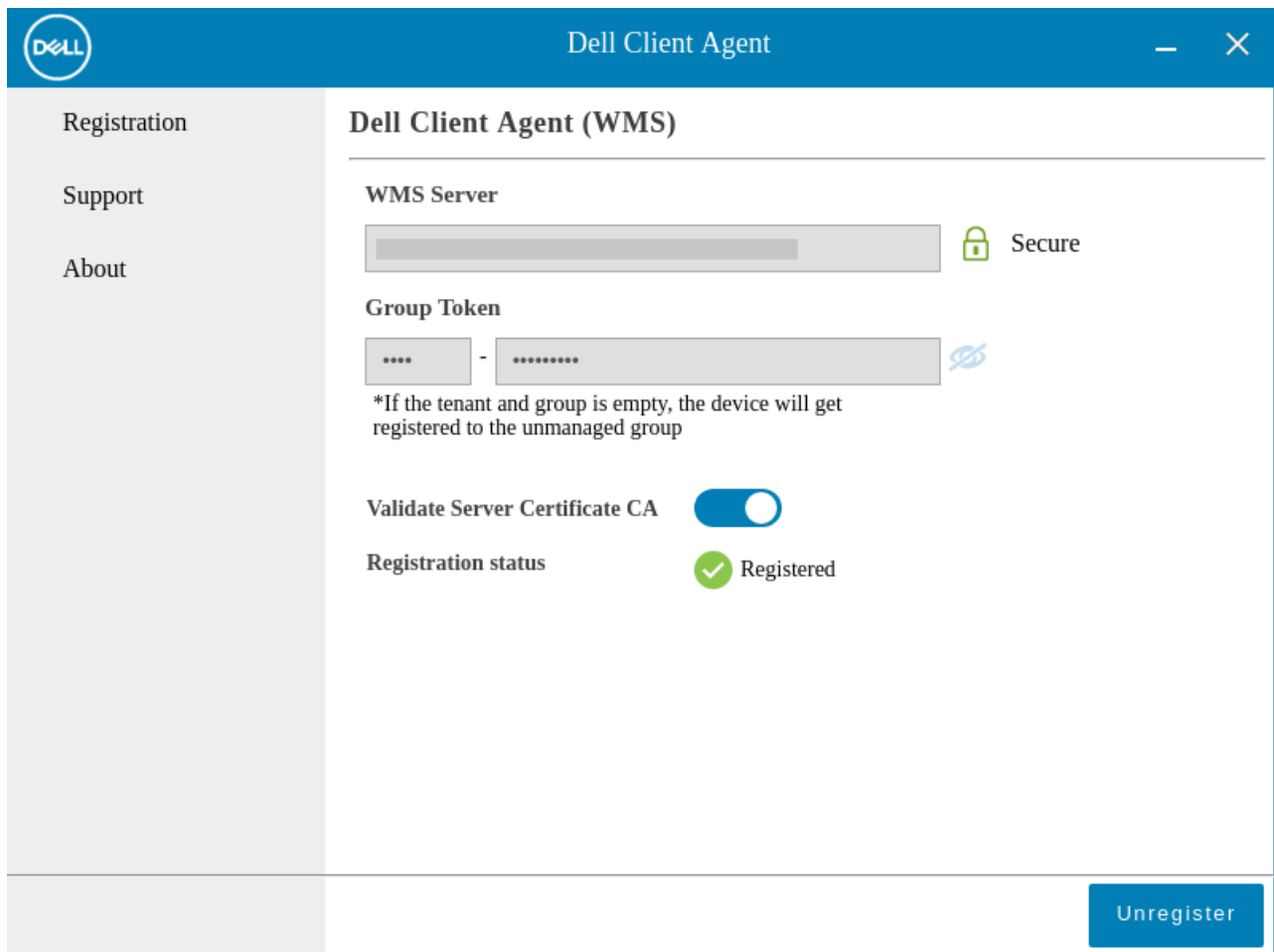
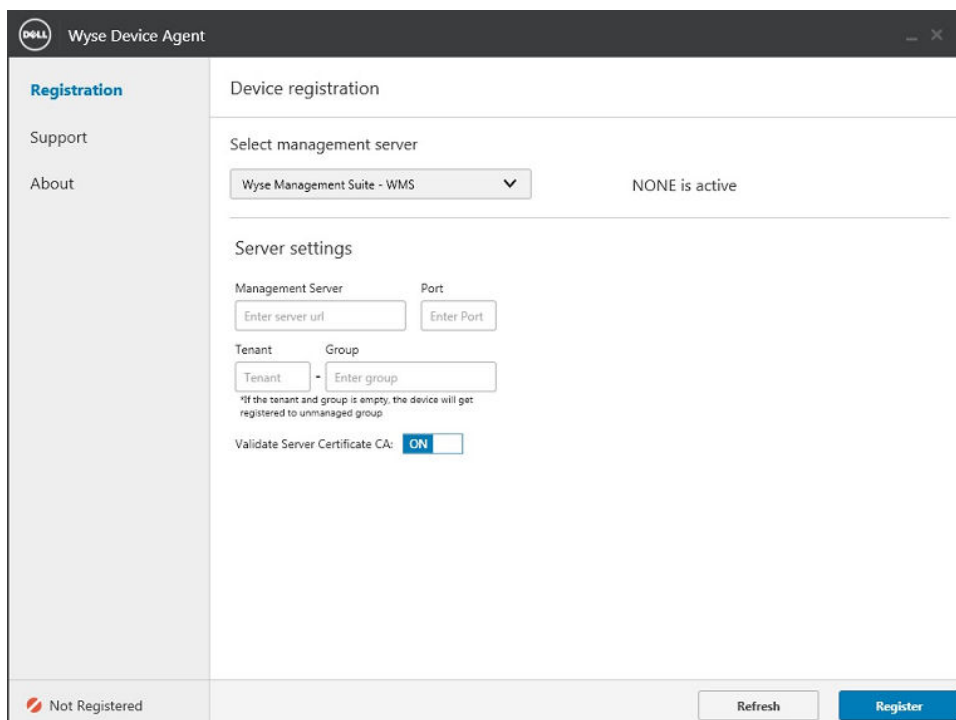


Figura 34. Dell Client Agent

# Registrazione manuale dei dispositivi Windows Embedded Standard

I dispositivi Windows Embedded Standard possono essere registrati manualmente avviando l'icona **IU WDA** sulla barra delle applicazioni.

1. Selezionare **Wyse Management Suite-WMS** come server di gestione.
2. Immettere un tenant appropriato e un nome gruppo. Se questo campo viene lasciato vuoto, i dispositivi vengono registrati in un gruppo non gestito. (opzionale)
3. Fare clic su **Registra**.



The screenshot shows the 'Wyse Device Agent' application window. On the left is a sidebar with 'Registration' (highlighted), 'Support', and 'About'. The main area is titled 'Device registration' and contains the following elements:

- Select management server:** A dropdown menu showing 'Wyse Management Suite - WMS' and the text 'NONE is active'.
- Server settings:**
  - Management Server:** 'Enter server url' and 'Enter Port' input fields.
  - Tenant and Group:** 'Tenant' and 'Enter group' input fields.
  - \*If the tenant and group is empty, the device will get registered to unmanaged group
  - Validate Server Certificate CA:** A toggle switch currently set to 'ON'.
- Status:** A red circle with a slash and the text 'Not Registered'.
- Buttons:** 'Refresh' and 'Register' buttons at the bottom right.

Figura 35. Registrazione del dispositivo

# Registrazione manuale del dispositivo ThinOS

## 8.x

### Procedura

1. Dal menu del desktop del thin client, andare su **Configurazione del sistema > Configurazione centrale**. Viene visualizzata la finestra **Configurazione centrale**.
2. Inserire la **Chiave di registrazione gruppo** come configurato dall'amministratore per il gruppo desiderato.
3. Selezionare la casella di controllo **Abilita impostazioni avanzate WMS**.
4. Nel campo **Server WMS**, inserire l'URL di Wyse Management Server.
5. Abilitare o disabilitare la convalida CA in base al tipo di licenza in proprio possesso. Per public cloud, selezionare la casella di controllo **Abilita convalida CA**. Per il cloud privato, selezionare la casella di controllo **Abilita convalida CA** se sono stati importati i certificati da un'autorità di certificazione nota al proprio server Wyse Management Suite.  
Per abilitare l'opzione di convalida CA nel private cloud, è necessario installare lo stesso certificato con firma automatica sul dispositivo ThinOS. Se il certificato con firma automatica non è stato installato sul dispositivo ThinOS, non selezionare la casella di controllo **Abilita convalida CA**. È possibile installare il certificato sul dispositivo utilizzando Wyse Management Suite dopo la registrazione, quindi abilitare l'opzione di convalida CA.
6. Per verificare la configurazione, cliccare su **Convalida codice**.
  - N.B.:** Se la chiave non è convalidata, verificare la chiave del gruppo e l'URL del server WMS forniti. Accertarsi che le porte indicate non siano bloccate dalla rete. Le porte predefinite sono 443 e 1883.
7. Cliccare su **OK**.
  - N.B.:** Una volta abilitata l'opzione di **Convalida iscrizione**, i dispositivi manuali o rilevati automaticamente sono in stato di **Convalida iscrizione in sospeso** nella pagina **Dispositivi**. Il tenant può selezionare un singolo dispositivo o più dispositivi nella pagina **Dispositivi** e convalidare l'iscrizione. Dopo la convalida, i dispositivi vengono spostati nel gruppo desiderato.


Il dispositivo viene registrato a Wyse Management Suite.

# Registrazione manuale del dispositivo ThinOS

## 9.x


### Procedura

1. Dal menu del desktop del thin client, andare su **Configurazione del sistema > Configurazione centrale**. Viene visualizzata la finestra **Configurazione centrale**.
2. Inserire la **Chiave di registrazione gruppo** come configurato dall'amministratore per il gruppo desiderato.
3. Selezionare la casella di controllo **Abilita impostazioni avanzate WMS**.
4. Nel campo **Server WMS**, inserire l'URL di Wyse Management Server.
5. Abilitare o disabilitare la convalida CA in base al tipo di licenza in proprio possesso. Per il public cloud, selezionare la casella di controllo **Abilita Convalida CA** e per il private cloud selezionare la casella di controllo **Abilita Convalida CA** se sono stati importati certificati da un'autorità di certificazione nota al proprio server Wyse Management Suite.  
Per abilitare l'opzione di convalida CA nel private cloud, è necessario installare lo stesso certificato con firma automatica sul dispositivo ThinOS. Se il certificato con firma automatica non è stato installato sul dispositivo ThinOS, non selezionare la casella di controllo **Abilita convalida CA**. È possibile installare il certificato sul dispositivo utilizzando Wyse Management Suite dopo la registrazione, quindi abilitare l'opzione di convalida CA.
6. Per verificare la configurazione, cliccare su **Convalida codice**.

 **N.B.:** Se la chiave non è convalidata, verificare la chiave del gruppo e l'URL del server WMS forniti. Accertarsi che le porte indicate non siano bloccate dalla rete. Le porte predefinite sono 443 e 1883.

Viene visualizzata una finestra di avviso.

7. Cliccare su **OK**.
8. Cliccare su **OK** nella finestra **Configurazione centrale**.

 **N.B.:** Una volta abilitata l'opzione di **Convalida iscrizione**, i dispositivi manuali o rilevati automaticamente sono in stato di **Convalida iscrizione in sospeso** nella pagina **Dispositivi**. Il tenant può selezionare un singolo dispositivo o più dispositivi nella pagina **Dispositivi** e convalidare l'iscrizione. Dopo la convalida, i dispositivi vengono spostati nel gruppo desiderato.

Il dispositivo viene registrato a Wyse Management Suite.

# Registrazione manuale dei dispositivi Linux

È possibile registrare manualmente i dispositivi Linux avviando l'icona **IU WDA** da **Impostazioni di sistema**.

1. Immettere i dettagli **Server WMS**.
2. Immettere un tenant appropriato e un nome gruppo. Se questo campo viene lasciato vuoto, i dispositivi vengono registrati in un gruppo non gestito. (opzionale)
3. Fare clic su **Registra**.

Il dispositivo viene registrato nella console Wyse Management Suite.

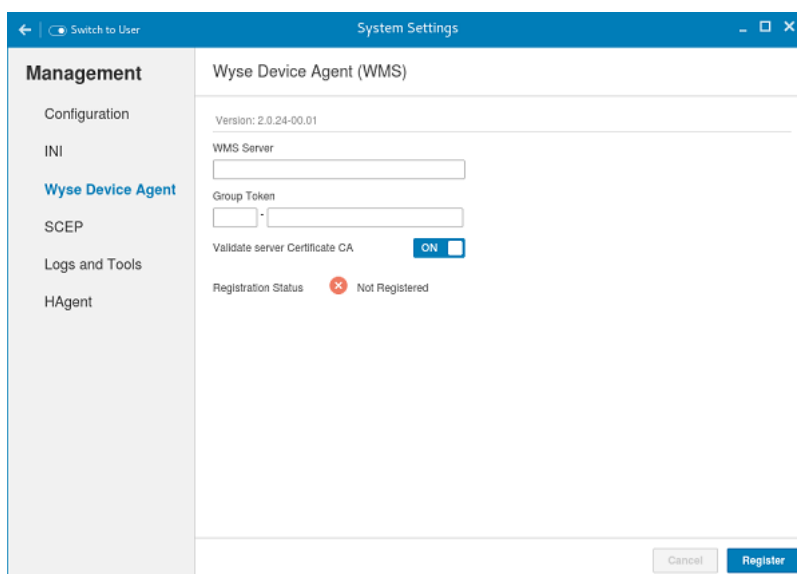


Figura 36. Registrazione del dispositivo



## Termini e definizioni

La tabella seguente elenca i termini che vengono utilizzati nel presente documento e le relative definizioni:

**Tabella 7. Termini e definizioni**

| <b>Terminologia</b>       | <b>Definizione</b>   |
|---------------------------|--|
| Private cloud             | Il server Wyse Management Suite installato sul cloud che è privato per il data center padre.   |
| WDA                       | Wyse Device Agent che risiede nel dispositivo e funge da agente per la comunicazione tra server e client.  |
| Repository locale         | Wyse Device Agent che risiede nel dispositivo e funge da agente per la comunicazione tra server e client.  |
| Repository remoto         | Applicazione, immagine del sistema operativo e repository di file che, se lo si desidera, possono essere installati per la scalabilità e l'affidabilità per le diverse aree geografiche per il trasferimento dei contenuti.  |
| Public cloud              | Wyse Management Suite in hosting su un public cloud con la convenienza e il risparmio sui costi legati al fatto di non dover configurare e gestire l'infrastruttura e il software.   |
| Componente aggiuntivo/app | Qualsiasi componente o pacchetto che non fa parte della build di base e fornito come componente opzionale. Il componente o il pacchetto può essere distribuito dal software di gestione. Ad esempio, gestori di connessioni più recenti con VMware e Citrix.   |
| On-premise                | Il server Wyse Management Suite installato on-premise che è privato per il data center dell'organizzazione.  |
| Tenant                    | Gruppo di utenti che condividono un accesso comune con privilegi specifici per Wyse Management Suite. Si tratta di una chiave univoca assegnata a clienti specifici per accedere alla suite di gestione.   |
| Utenti                    | Gli utenti possono essere amministratori locali, amministratori globali e visualizzatori. Agli utenti di gruppo e a quelli importati da Active Directory è possibile assegnare ruoli di amministratore globale, amministratore di gruppo e visualizzatore per accedere a Wyse Management Suite. Agli utenti vengono fornite le autorizzazioni per eseguire operazioni in base ai ruoli loro assegnati. |