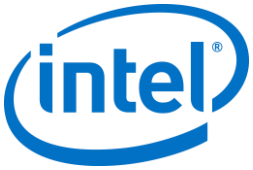
Soluzione Intel Unite®

Guida per l'implementazione aziendale

Maggio 2017



Esclusioni di responsabilità legale e copyright

Sommario

1 Introduzione

Il software Intel Unite® rende possibili ambienti per riunioni sicuri e connessi per una collaborazione semplificata. È stato studiato per connettere tutti i partecipanti di una riunione in modo semplice e rapido. La soluzione Intel Unite, oggi disponibile, rende la collaborazione semplice e istantanea e rappresenta un punto di partenza a cui in futuro si aggiungeranno nuove funzionalità e caratteristiche.
Questo documento serve per installare il software Intel Unite in modalità Enterprise, ne spiega meglio le funzioni ed è d'aiuto per la risoluzione dei problemi.

1.1 Destinatari

Il documento è destinato ai professionisti IT degli ambienti aziendali e ad altri destinatari che implementeranno la soluzione Intel Unite in un ambiente aziendale.

1.2 Terminologia e definizioni della soluzione Intel Unite

Server Enterprise (server): questo termine si riferisce al server Web e al servizio PIN in esecuzione sul server che assegnerà e risolverà i PIN. Offre una pagina di download per i client e il portale di amministrazione per la configurazione.

Client: questo termine si riferisce a un dispositivo (Windows*, macOS*, iOS*, Android* o Chromebook*) utilizzato per connettersi all'hub.

Hub: questo termine si riferisce a un PC mini con tecnologia Intel® vPro™ collegato a un display della sala conferenze sul quale viene eseguita l'applicazione Intel Unite.

FQDN: acronimo di Fully Qualified Domain Name, ossia nome di dominio completo.

Plug-in: questo termine si riferisce a un componente software installato sull'hub che estende le funzionalità della soluzione Intel Unite.

IIS: acronimo di Internet Information Services, un server Web fornito da Microsoft*.

1.3 Novità della soluzione Intel Unite

Per agevolare l'individuazione delle caratteristiche aggiunte alla soluzione, nella tabella seguente sono riepilogate le nuove funzioni introdotte a partire dalla versione 1.0.

v 2.0	v 3.0	v 3.0 MR	v 3.1
Schermo esteso	Hardware con streaming audio/video accelerato per Windows (1080 @20-30fps)	Supporto di iOS per le presentazioni	Esperienza utente ottimizzata per il portale di amministrazione: aspetto diverso con l'aggiunta di finestre di dialogo che agevolano la selezione delle impostazioni
Supporto di Windows 10	Plug-in per l'accesso guest protetto		Portale di amministrazione: Pianifica riunione
Plug-in per l'accesso degli utenti guest	Riunioni pianificate (sala singola)		Portale di amministrazione: modalità Moderatore
Plug-in per Skype for Business	Blocco riunione		Portale di amministrazione: PIN statico
	Supporto di iOS per la visualizzazione		Portale di amministrazione: Prenotazione PIN
			Portale di amministrazione: Trasparenza del PIN
			Portale di amministrazione: Disattiva visualizzazione remota
			Supporto di Chrome OS
			Supporto di Android

2 Requisiti della soluzione Intel Unite

2.1 Requisiti del server Enterprise

- Microsoft Windows* Server 2008 o versione successiva
- Microsoft Internet Information Services con abilitazione per SSL
    - È richiesto un certificato del server Web basato su SHA2 attendibile con una radice di attendibilità pubblica o interna
- Server di posta elettronica SMTP configurato in Microsoft Internet Information Services
- Microsoft SQL Server 2008 R2 o versione successiva
- Microsoft .NET* 4.5 o versione successiva
- 4 GB di RAM
- 32 GB di storage disponibile
  NOTA: il server Web IIS e il server database Microsoft SQL possono essere installati su computer diversi

2.2 Requisiti dell'hub

- Microsoft Windows 7 SP1, 8.1 o 10 (32 bit e 64 bit)
    - Ultimo livello di patch consigliato
- Microsoft .NET 4.5 o versione successiva
- SKU supportati[1], mini PC con processore Intel® Core™ vPro™ di quarta generazione o successive
- Connessione di rete cablata o wireless
- 4 GB di RAM
- 32 GB di storage disponibile

2.3 Requisiti del client

- Microsoft Windows 7 SP1, 8.1 o 10 (32 bit e 64 bit)
    - Ultimo livello di patch consigliato
- Microsoft .NET 4.5 o versione successiva
- OS X* 10.10.5 e versione successiva
- iOS 9.3 o versione successiva
- Connessione di rete cablata o wireless

[1] Per gli SKU supportati, rivolgersi al produttore dell'hardware originale o a un rappresentante Intel

2.4 Requisiti di rete e considerazioni in ambito IT

L'installazione dell'hub e del client deve essere gestita secondo le procedure stabilite dal reparto IT per la distribuzione del software.
Per una maggiore affidabilità, si consiglia di utilizzare una connessione di rete cablata per l'hub. In questo modo è possibile evitare la saturazione della larghezza di banda wireless, soprattutto nelle aree soggette a traffico congestionato.
Un altro aspetto da considerare è la necessità di configurare il software Intel Unite in modo che accetti le connessioni in ingresso. A tale scopo l'utente deve aggiungere un'eccezione al firewall installato sull'hub. Contattare il produttore del firewall per informazioni specifiche su come creare eccezioni di applicazioni.

In un ambiente di produzione, si consiglia di utilizzare un nome di dominio completo (FQDN) e di configurare un record di servizio DNS che faccia riferimento al server Enterprise. Si tratta del metodo più semplice con cui gli hub e i client possono individuare il server Enterprise.
Come ulteriore misura di sicurezza, l'applicazione accetta solo certificati SHA-2 o successivi. Pertanto, è possibile che venga richiesto di aggiornare i certificati sul server Web. Consultare il team di sicurezza IT per ottenere i certificati SHA-2 durante la configurazione.

2.4.1 Dispositivi client mobili

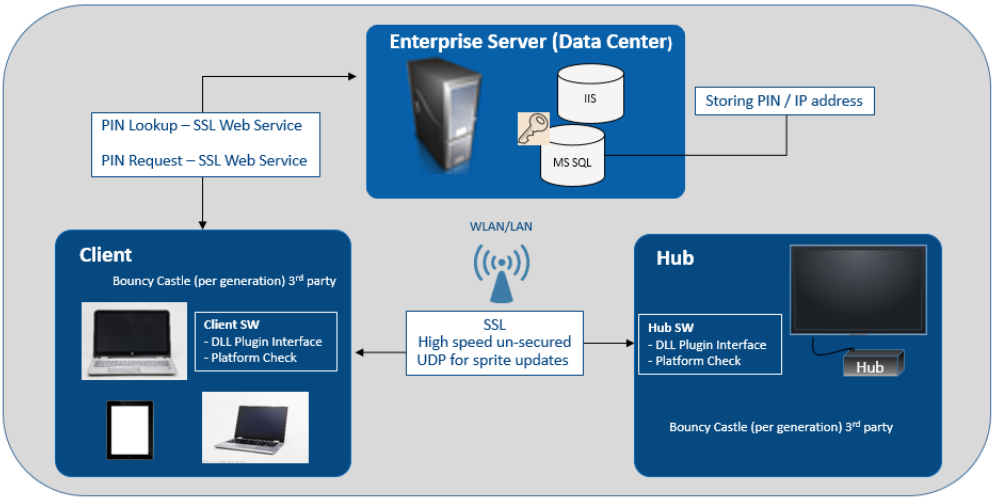
Se l'organizzazione prevede di distribuire dispositivi client mobili come parte dei sistemi operativi client Intel Unite, tenere presente quanto segue:
Per potersi connettere alla soluzione Intel Unite, tutti i dispositivi client devono essere connessi alla rete aziendale oppure utilizzare una VPN opportunamente configurata. Sono inclusi i dispositivi iOS e Android. I tablet e i telefoni, normalmente impiegati per uso personale, che non sono connessi alla rete aziendale ma a quella del proprio gestore potrebbero non essere in grado di connettersi a una sessione dell'app Intel Unite per via di un firewall aziendale che non consente queste connessioni.

Per gli amministratori IT:

- Se gli utenti dell'app Intel Unite utilizzano i propri dispositivi mobili, per consentire la connessione a Intel Unite è necessario verificare che essi siano connessi alla rete aziendale oppure creare un metodo per consentire queste connessioni.
- Assicurarsi di avere gli strumenti necessari per gestire correttamente questi dispositivi e mantenere la rete sicura.
- Stabilire una strategia appropriata per la gestione di questi dispositivi, che potrebbero aggiungere ulteriori rischi per la sicurezza.
- Stabilire dei criteri per la gestione dei dispositivi mobili personali o per uso lavorativo.
- La sicurezza deve essere adattata per fornire il giusto livello di protezione, secondo la sensibilità dei dati da tutelare. Il livello di adattamento dipende dai dati che l'azienda considera critici e da quanto capillarmente questa sia disposta ad applicare le protezioni.

3 Panoramica sull'implementazione

La soluzione Intel Unite è formata da tre componenti: un server Enterprise, un hub e un client.
Il server Enterprise è il primo componente da configurare. Quando verranno avviate le applicazioni dell'hub e del client, il server Enterprise servirà per scambiare informazioni sulla connessione e ricevere le assegnazioni del PIN.
L'hub è il mini PC con processore Intel Core vPro che solitamente è connesso a un display o a un proiettore in una sala conferenza.
I client seguono le istruzioni visualizzate sull'hub per scaricare il software necessario e connettersi all'hub inserendo il PIN visualizzato. Una volta connesso, un client può presentare, visualizzare e annotare i contenuti e condividere file con gli altri partecipanti connessi allo stesso hub, interagendo con i plug-in installati su quest'ultimo.
In questo diagramma è raffigurata una panoramica dei componenti installati.



3.1 Risorse di implementazione

Per completare l'installazione, è necessario disporre di quanto segue:

- Diritti amministrativi sul database
- Diritti amministrativi sul server Enterprise
- Diritti amministrativi sull'hub

Potrebbero inoltre servire:

- L'amministratore della sicurezza IT per emettere il certificato SHA-2
- Amministratore della sicurezza IT per i criteri dei firewall
- Amministratore IT in grado di creare un record del servizio DNS, utilizzato dall'hub e dai client per individuare il server Enterprise (vivamente consigliato)

4 Installazione del server Enterprise

4.1 Panoramica del server Enterprise

Il programma di installazione del server Enterprise include il database, il server PIN, il portale Web di amministrazione e la pagina di download del client.
Il server Enterprise contiene 4 componenti:

1) Database Microsoft SQL: gestisce tutte le informazioni sullo stato per l'infrastruttura della soluzione Intel Unite.
2) Servizio Web: è un servizio di messaggistica standardizzato che comunica con il database e con gli hub e i client.
3) Sito Web del portale di amministrazione: consente di gestire gli hub e i client, genera statistiche e fornisce funzioni di monitoraggio e avviso.
4) Pagina Web di destinazione per il download del client: contiene il software Intel Unite per il client.

Inoltre, è importante sapere che gli hub e i client individuano il server Enterprise nell'infrastruttura di rete con uno di questi due metodi: file ServerConfig.xml o record di servizio DNS.
È consigliabile optare per il record di servizio DNS, in quanto consente di configurare il client e l'hub in modo del tutto automatico. Consultare la sezione relativa alla Creazione di un record di servizio DNS. Se non è possibile acquisire un record di servizio DNS, il server Enterprise può essere configurato nel file ServerConfig.xml. Consultare l'Appendice B per un Esempio di un file ServerConfig.xml.

4.2 Pre-installazione del server Enterprise

- Verificare che il server soddisfi i requisiti software e hardware minimi specificati.
- Verificare che nel server sia installato IIS versione 8.0 o successiva. Il programma di installazione del server richiede che i servizi IIS siano attivi, altrimenti non sarà possibile procedere. Per informazioni sull'attivazione e sulla configurazione IIS, vedere la sezione Attivazione IIS.
- Configurare il server di posta elettronica SMTP in IIS Manager, vedere la sezione
- Impostazioni del server di posta elettronica.
- Verificare di aver installato e attivato ASP.NET 4.5.
- Verificare che SSL sia attivato in IIS (i siti https dovrebbero funzionare). **NOTA:** a tale scopo potrebbe essere necessario richiedere la collaborazione del reparto IT per installare un certificato SHA-2 con una radice di attendibilità valida.
- Assicurarsi di disporre dell'accesso amministrativo a Microsoft SQL tramite l'autenticazione di Windows o l'autenticazione di SQL. Vedere la sezione Installazione di Microsoft SQL Server.
- Aggiungere un record del servizio DNS per attivare la ricerca automatica del server Enterprise. Consultare la sezione relativa alla Creazione di un record di servizio DNS.

4.2.1 Aggiornamento del software

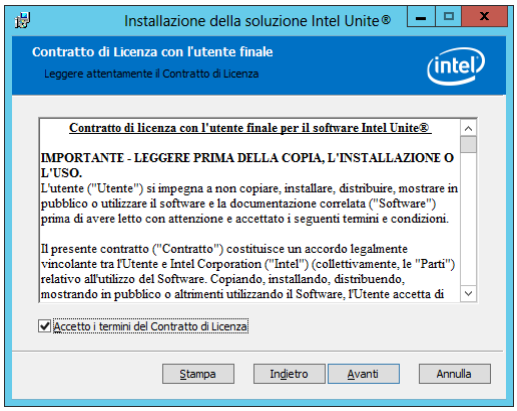
Se la propria organizzazione sta eseguendo un aggiornamento del software:

- Assicurarsi di eseguire il backup del database, poiché le modifiche non possono essere annullate.
- Tutte le connessioni al database devono essere chiuse prima di eseguire l'aggiornamento (disconnettersi dal portale di amministrazione)
- Durante l'aggiornamento, l'opzione Database è selezionata per impostazione predefinita - per l'installazione sia locale che remota - quando Intel Unite server.msi è in esecuzione sul server Pin.

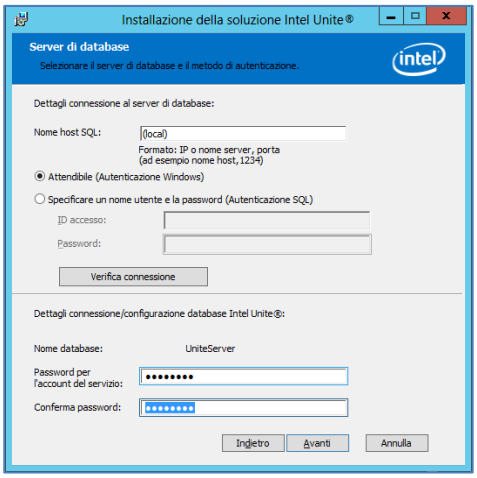
4.3 Installazione del server Enterprise

Dopo aver verificato tutti i passaggi descritti nella sezione precedente (Pre-installazione del server Enterprise), continuare con i programmi di installazione del software Intel Unite (questo processo deve essere eseguito sul server che ospita l'ambiente IIS).

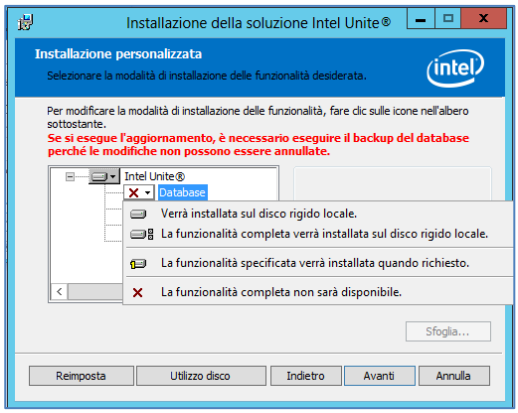
- Individuare il file **Intel Unite Server.mui.msi** e fare doppio clic per installare il/i server di destinazione.
- L'installazione guidata offre la possibilità di installare i componenti seguenti: un database, un servizio Web, una pagina di download del client e un portale di amministrazione.
- Dopo l'avvio di **Intel Unite Server.mui.msi**, accettare il Contratto di Licenza, selezionando la casella **Accetto i termini del Contratto di Licenza**.

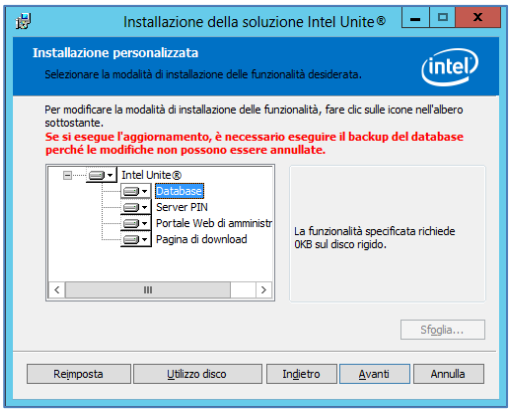


- Fare clic su **Avanti** per andare alla finestra Server database.
- Nella finestra Server database, selezionare **Dettagli connessione al server di database**. Le opzioni disponibili sono:
  - Nella casella **Nome host SQL**, il valore predefinito di SQL server è **(locale)**. È possibile cambiarlo modificando il nome oppure lasciare il valore predefinito **(locale)** se SQL è installato sullo stesso server.
  - Il valore predefinito per il server è **Attendibile (autenticazione Windows)** (se è già stato eseguito l'accesso) oppure selezionare **Specificare nome utente e password (autenticazione SQL)** se si dispone di credenziali valide che consentono l'accesso al database e se si preferisce l'autenticazione SQL. Se si sceglie quest'ultima opzione, assicurarsi di TESTARE prima la connessione del database facendo clic su **Verifica connessione**.
  - Nella sezione **Dettagli connessione/configurazione database**, è necessario creare una password per **UniteServiceUser**, utilizzato per accedere al nuovo database UniteServer. Nella casella successiva, selezionare **Confermare password**.
  - La password deve contenere almeno 8 caratteri, almeno una lettera maiuscola, una lettera minuscola, un numero e un simbolo.



- Fare clic su **Avanti** per passare alla finestra **Installazione personalizzata** per la selezione delle funzionalità. Espandere la funzionalità Database e selezionare una delle funzionalità **Verrà installata sul disco rigido locale** o **La funzionalità completa verrà installata sul disco rigido locale**. Il Database viene così creato nell'SQL server specificato nel passaggio precedente.

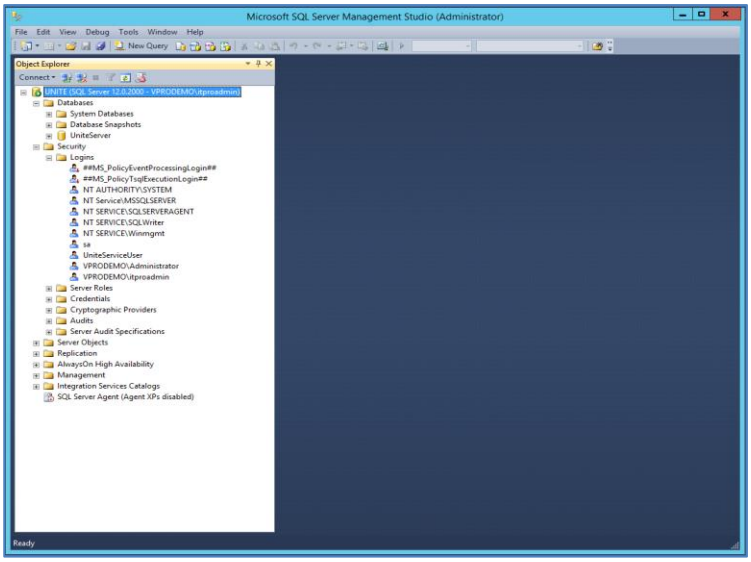




- Fare clic su **Avanti** per verificare la selezione della funzionalità e iniziare con l'installazione facendo clic su **Installa**.
- Fare clic su **Fine** per completare l'installazione.
- Il server Enterprise è stato installato. Continuare con la sezione successiva per installare l'hub.

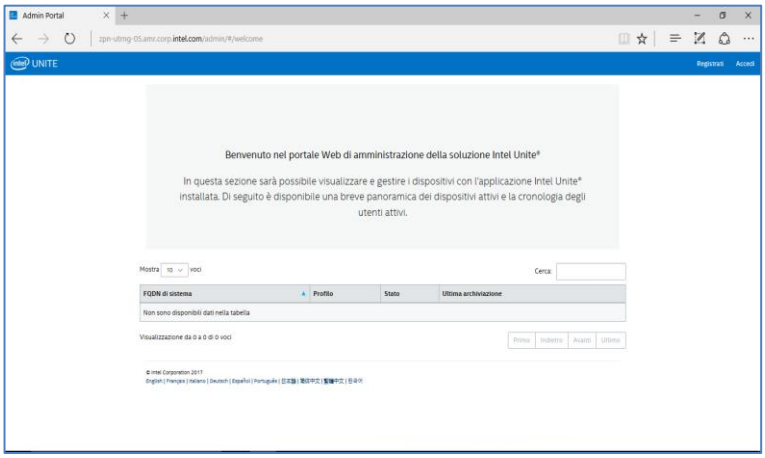
Facoltativo:

- Per verificare che il database UniteServer sia stato creato utilizzando SQL Management Studio, aprire SQL Management Studio sul server e connettersi a SQL server. Espandere i database nel riquadro a sinistra e verificare l'avvenuta creazione del database UniteServer.



- Verificare che l'installazione sia stata completata eseguendo l'accesso al portale di amministrazione (se installato sul server insieme al database e al server PIN) con il seguente collegamento:
  https://<nomeserver>/admin

Effettuare l'accesso al proprio account o utilizzare l'account di amministratore predefinito (per l'installazione di un nuovo software):
Utente: admin@server.com
Password: Admin@1

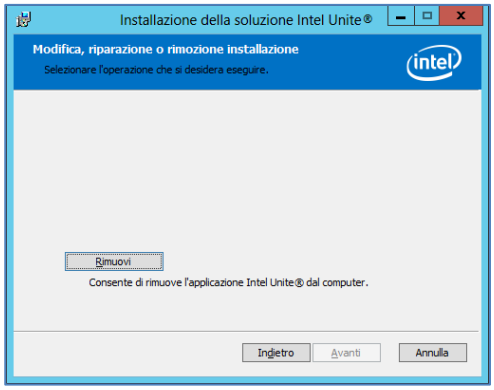


Nota: se si riceve un messaggio di errore durante l'accesso al portale di amministrazione, consultare la sezione Risoluzione dei problemi.

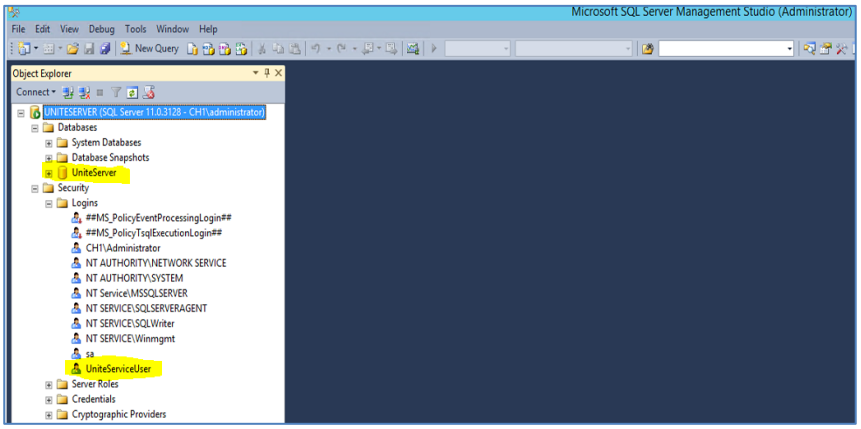
4.4 Disinstallazione dell'applicazione Intel Unite

Se si deve disinstallare l'applicazione, è necessario eliminare anche il database UniteServer e l'accesso UniteServiceUser creato in precedenza per evitare conflitti all'interno dell'applicazione. Prima di eseguire questa operazione, **assicurarsi di aver creato una copia di backup del database**.

1. Avviare il programma di installazione **Intel Unite Server.mui**.
2. Fare clic su **Rimuovi** e quindi su **Avanti** per continuare.



3. Accedere a *Microsoft SQL Server Management Studio* ed eliminare manualmente il database SQL **UniteServer** e l'account **UniteServiceUser**. Vedere le aree evidenziate nell'immagine qui in basso.


Microsoft SQL Server Management Studio (Administrator)
File Edit View Debug Tools Window Help
New Query
Object Explorer
Connect
UNITESERVER (SQL Server 11.0.3128 - CH1\administrator)
Databases
System Databases
Database Snapshots
UniteServer
Security
Logins
##MS_PolicyEventProcessingLogin##
##MS_PolicyTsqlExecutionLogin##
CH1\Administrator
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM
NT Service\MSSQLSERVER
NT SERVICE\SQLSERVERAGENT
NT SERVICE\SQLWriter
NT SERVICE\Winmgmt
sa
UniteServiceUser
Server Roles
Credentials
Cryptographic Providers

5 Installazione dell'hub

5.1 Pre-installazione dell'hub

L'applicazione Intel Unite richiede la creazione di un'esclusione nel firewall dell'hub per poter eseguire l'accesso e comunicare con il server Enterprise, dal momento che l'hub deve essere in grado di individuare e accedere al server Enterprise.
Quando si esegue il programma di installazione dell'hub, vengono richiesti i dettagli della connessione al server e viene data la possibilità di saltare la ricerca manuale (denominata **Specifica il server** nel processo di installazione) e di utilizzare invece il recupero di informazioni dal record del servizio DNS. Durante l'esecuzione del programma di installazione dell'hub, viene modificato il file ServerConfig.xml.
A seconda del metodo scelto per la ricerca del PIN, è necessario sapere se utilizzare la selezione **Trova server automaticamente** o **Specifica il server** durante l'esecuzione dell'installazione.
Se è certi dell'esistenza di un record del servizio DNS, è possibile selezionare **Trova server automaticamente**. In caso di dubbio, utilizzare l'**opzione Specifica il server** (ricerca manuale), in cui è richiesto di conoscere il nome host per il server Enterprise.
Se è stato modificato il file ServerConfig.xml con la chiave pubblica (vedere la sezione successiva Chiave pubblica), non è necessario immettere nuovamente la chiave per i programmi di installazione del client e dell'hub.
Nota: se un server è definito nel file ServerConfig.xml, questo avrà precedenza sul record del servizio DNS.

5.1.1 Chiave pubblica

La chiave pubblica è opzionale; la sua funzione è quella di specificare in che modo l'hub o il client comunica con il server Enterprise. Se il campo è vuoto o non è specificata alcuna chiave, l'hub e il client convalidano la radice di attendibilità. Se l'applicazione non accetta il certificato, viene richiesto l'utente.

La chiave pubblica viene utilizzata quando si esegue l'installazione dell'hub e del client. È richiesta quando si eseguono i programmi di installazione dell'hub e del client. Per ottenere la chiave pubblica, visitare il sito: https://yourservername/unite/ccservice.asmx

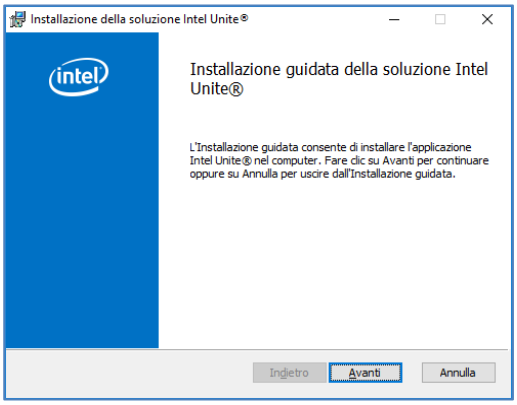
Nella barra dell'URL, fare clic sull'icona del lucchetto per visualizzare le informazioni sul certificato. Andare ai dettagli, fare clic su Mostra tutti, scorrere verso il basso fino al campo “Chiave pubblica”, quindi fare clic sulla chiave per visualizzarla. A questo punto, è possibile copiare il valore e incollarlo nel file ServerConfig.xml.

Assicurarsi di rimuovere gli spazi della stringa dopo averla incollata nel file ServerConfig. Se è stato modificato il file ServerConfig.xml con la chiave pubblica, non è necessario immettere nuovamente la chiave per i programmi di installazione del client e dell'hub. Consultare l'Appendice B per un Esempio di un file ServerConfig.xml.

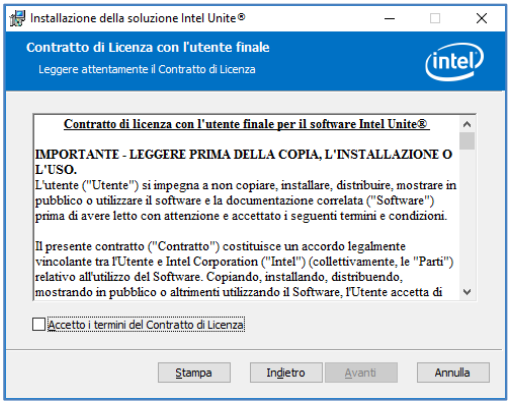
5.2 Installazione dell'hub

- Individuare la cartella del programma di installazione ed eseguire il file di installazione dell'hub: **Intel Unite Hub.mui.msi**

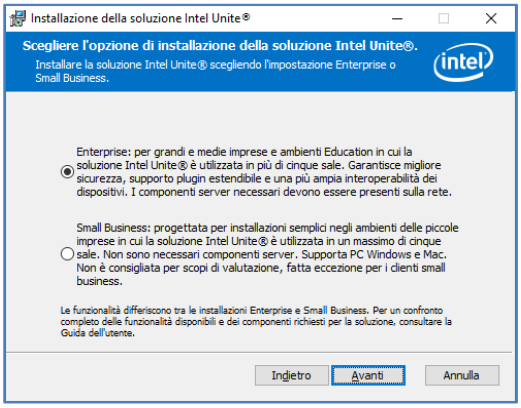
- Fare clic su **Avanti** per continuare.



- Fare clic su **Avanti** dopo aver selezionato la casella **Accetto i termini del Contratto di Licenza**.

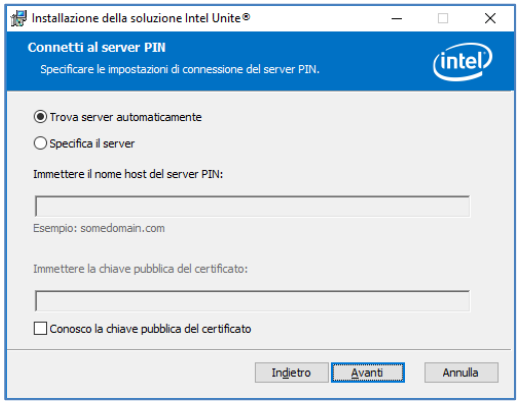


- Scegliere **Enterprise** e fare clic su **Avanti**.

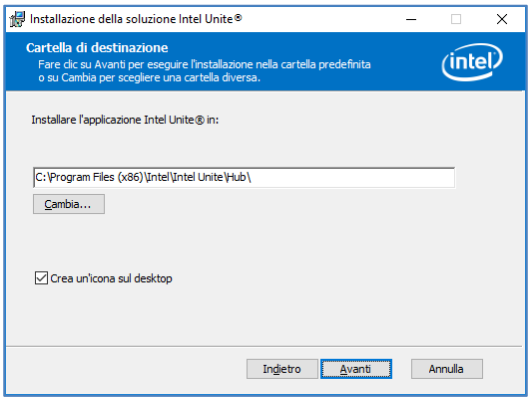


- In questa finestra, specificare le impostazioni di connessione del server PIN; sono disponibili le seguenti opzioni:
  - **Trova server automaticamente**: si tratta dell'opzione consigliata (impostazione predefinita).
  - **Specifica il server**: in questo passaggio, è necessario conoscere il nome host per il server Enterprise
    - **Immettere il nome host del server PIN.**
    - Immettere la **chiave pubblica del certificato** se è stato selezionato **Conosco la chiave pubblica del certificato**.

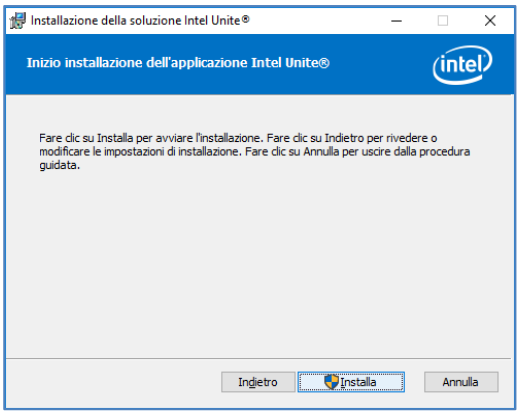
  Selezionare l'opzione e fare clic su **Avanti**.



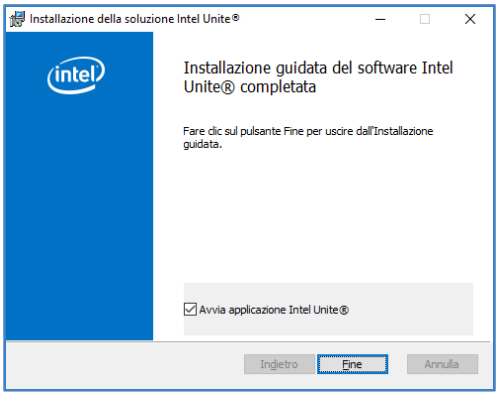
- La finestra **Cartella di destinazione** si apre in corrispondenza della cartella predefinita in cui verrà installato l'hub. Se lo si desidera, è possibile modificare la cartella di destinazione. Altrimenti mantenere la posizione predefinita. In questo passaggio, è inoltre possibile creare un'icona sul desktop. Fare clic su **Avanti** per continuare.



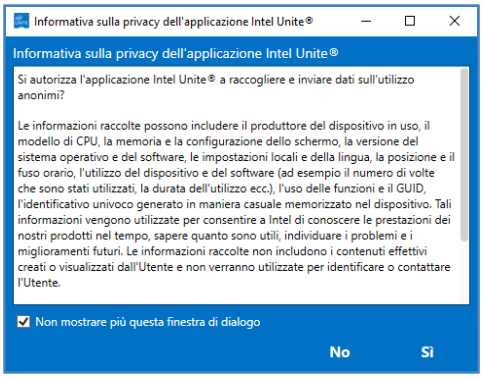
- Per rivedere le impostazioni, è possibile tornare indietro; per continuare, fare clic su **Installa**.



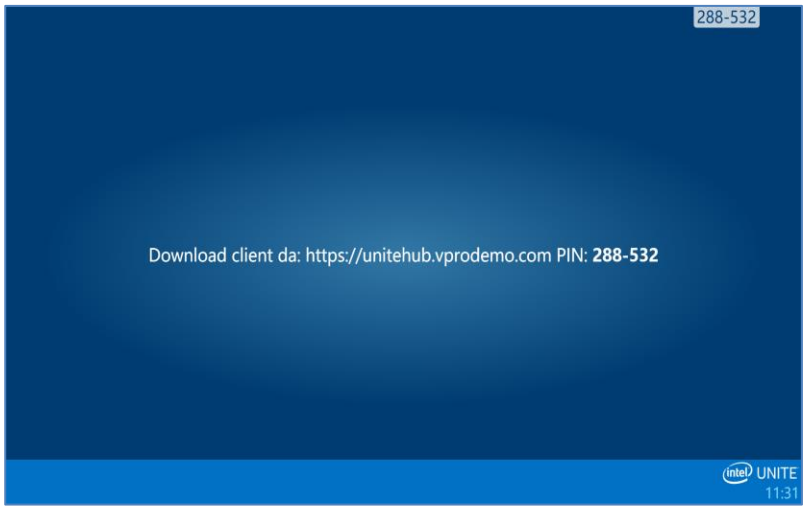
- Alla fine dell'installazione, viene visualizzata la finestra **Wizard dei installazione del software Intel Unite® completato**. Fare clic su **Fine** per completare il processo di installazione.



  - Quando l'applicazione viene avviata per la prima volta, viene visualizzata la **Dichiarazione sulla privacy dell'applicazione Intel Unite®**.



  - La funzione Dichiarazione sulla privacy dell'applicazione Intel Unite® viene utilizzata per raccogliere i dati sull'utilizzo anonimi. Intel è costantemente impegnata a migliorare i propri prodotti e per questo raccoglie i dati dei propri utenti. Selezionare **SÌ** o **NO** e selezionare la casella se non si desidera visualizzare la finestra di dialogo in futuro.
  - Sullo schermo o sul monitor, è ora visualizzato un codice PIN. Si tratta del PIN che serve ai client per la connessione all'hub. Consultare la sezione Risoluzione dei problemi se il PIN non viene visualizzato.



5.3 Configurazione dell'hub

Le opzioni di configurazione per gli hub che eseguono il software Intel Unite possono essere modificate attraverso il portale di amministrazione. Nel portale di amministrazione è presente un profilo predefinito con impostazioni di configurazione predefinite, applicate a tutti gli hub che eseguono l'archiviazione con il server Enterprise. Quando viene stabilita una connessione dall'hub al server Enterprise, viene eseguito il push delle opzioni di configurazione nell'hub. Le impostazioni vengono aggiornate ogni volta che l'hub effettua l'archiviazione. Nella maggior parte dei casi possono essere personalizzate in base alle esigenze della propria organizzazione; ad esempio, ogni hub può avere un colore diverso, un'immagine diversa o dimensioni diverse del PIN, contenere plug-in differenti e così via.
Per ulteriori informazioni sulla configurazione dell'hub, consultare la sezione Guida al portale di amministrazione.

5.4 Procedure consigliate per l'hub

Al fine di garantire la migliore esperienza possibile per l'utente finale, l'hub deve essere configurato in modo da essere sempre pronto all'uso e da sopprimere gli avvisi e i pop-up di sistema visualizzati sullo schermo. Le procedure consigliate includono le seguenti:

- Windows deve effettuare automaticamente l'accesso al dominio o all'account utente che verrà utilizzato dall'applicazione Intel Unite.
- Gli screen saver devono essere disabilitati.
- Il sistema deve essere impostato per non passare mai alla modalità di standby.
- Il sistema deve essere impostato per non eseguire mai la disconnessione.
- Il display deve essere impostato per non spegnersi mai.
- Gli avvisi di sistema devono essere soppressi.

5.5 Sicurezza dell'hub

L'amministratore dell'hub deve assicurarsi che le procedure di sicurezza consigliate vengano seguite per ogni hub. Se l'utente si connette automaticamente, verificare che non disponga di privilegi amministrativi.

5.6 Plug-in

L'applicazione Intel Unite supporta l'uso dei plug-in. I plug-in sono componenti software che estendono le caratteristiche e le funzioni dell'applicazione, implementando le varie modalità dell'esperienza utente. Ogni hub può essere dotato di plug-in univoci.
I seguenti plug-in sono attualmente disponibili per l'applicazione Intel Unite:

Plug-in per l'accesso guest protetto: questo plug-in consente a un computer di connettersi a un hub senza dover essere sulla stessa rete e senza la convalida PIN del server Enterprise. L'hub crea una rete in hosting/ad hoc (punto di accesso) alla quale può connettersi un client Intel Unite.

Plug-in per Skype for Business: questo plug-in è una soluzione per includere persone da una riunione Skype online in una sessione dell'app Intel Unite. Il plug-in viene eseguito sull'hub del software Intel Unite e gestisce un account di posta specifico per ciascuna istanza.

Plug-in di telemetria: se installato nell'hub, questo plug-in consente di aggiungere la possibilità per il server Enterprise di accettare e visualizzare i dati dell'hub. Il requisito minimo è Server Enterprise v3.0 (build N. 3.0.38.44).

Inoltre è disponibile un SDK per la scrittura dei plug-in:

Software Development Kit (SDK): guida all'interfaccia dell'applicazione utilizzata dagli sviluppatori del software o da chiunque cerchi di sviluppare funzionalità aggiuntiva per l'applicazione Intel Unite.

Nota: fare riferimento alle guide specifiche dei plug-in se si desidera installare o trovare altre informazioni su ciascun componente plug-in.

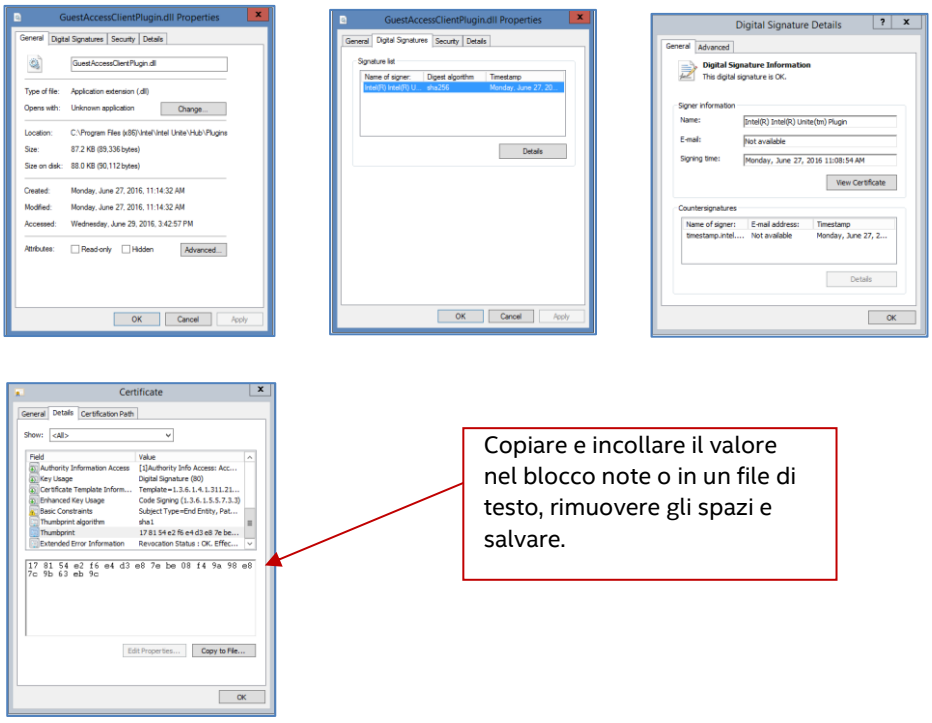
5.6.1 Note sull'installazione dei plug-in

Per impostazione predefinita, la posizione di installazione di ogni plug-in è la directory dei plug-in all'interno della directory di installazione [Program Files(x86) \Intel\Intel Unite\Hub\Plugins\PluginName (Plugin.dll)]. I plug-in vengono enumerati all'avvio dell'applicazione. Se si aggiunge un nuovo plug-in, è necessario riavviare l'applicazione.
Prima di installare il plug-in, verificare la compatibilità con la versione di destinazione della soluzione Intel Unite [consultare la guida specifica del plug-in, in quanto i requisiti variano tra plug-in].
È inoltre necessario ottenere e aggiungere il valore hash del certificato del plug-in nel portale Web di amministrazione per ciascun plug-in utilizzato.
NOTA: per un ambiente di test è possibile utilizzare il valore di chiave predefinito, ma non è consigliabile per un ambiente di produzione.

5.6.2 Valore hash del certificato del plug-in

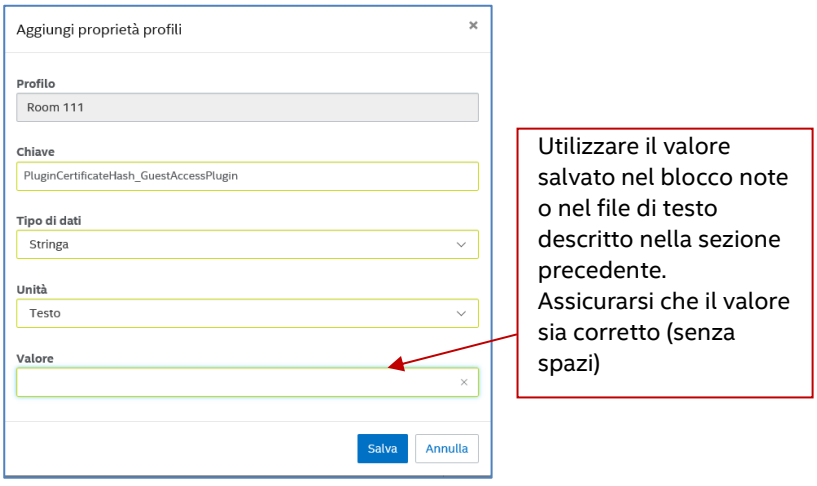
Attenersi alla seguente procedura per trovare il valore della chiave hash del certificato per il plug-in:

- Individuare il plug-in nella cartella Plug-in, fare clic con il pulsante destro del mouse su ***Plugin.dll** e scegliere **Proprietà** (ad esempio, GuestAccessClientPlugin.dll)
- All'apertura della finestra **Proprietà** del plug-in, individuare la scheda **Firme digitali**, quindi fare clic per aprirla.
- Selezionare **Plug-in Intel Unite** e fare clic su **Dettagli**.
- Nella finestra **Dettagli firma digitale**, fare clic su **Visualizza certificato.**
- Nella finestra **Certificato** selezionare la scheda **Dettagli** e scorrere in basso fino a visualizzare **Identificazione personale**.
- Una volta visualizzato il valore, selezionare **Identificazione personale**, copiarlo e incollarlo nel blocco note o in un file di testo, rimuovere gli spazi e salvare.
- Il valore della chiave verrà utilizzato in fase di creazione del profilo per il plug-in. È possibile crearlo e immetterlo dopo la creazione del profilo. Per ulteriori informazioni, passare alla sezione successiva.



5.6.3 Aggiunta dell'hash certificato a un plug-in nel portale Web di amministrazione

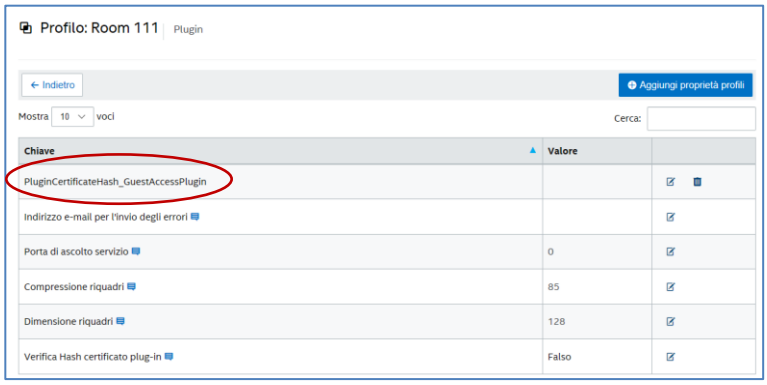
Accedere al portale Web di amministrazione. Nella pagina **Gruppi,** selezionare il profilo in cui attivare il plug-in.
Nella finestra Profilo, fare clic su **Aggiungi proprietà profili** e immettere quanto segue:



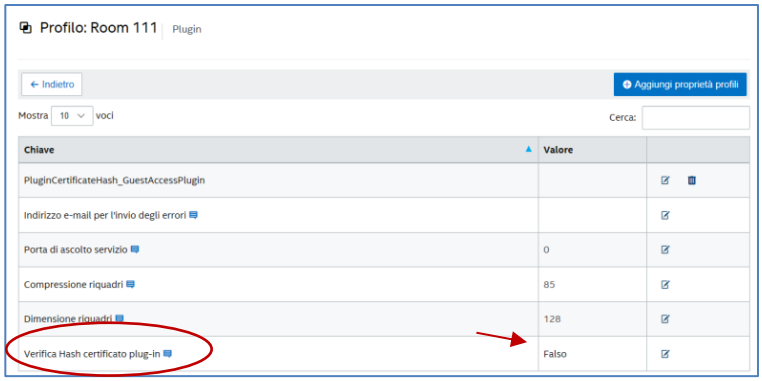
- **Chiave**: PluginCertificateHash_XXX
  - XXX è il nome del plug-in per il quale viene aggiunto il valore hash, ad esempio GuestAccessPlugin. Per semplificare l'identificazione, si consiglia di utilizzare il nome del plug-in che corrisponde all'hash.
- **Tipo di dati:** stringa
- **Unità:** testo

- **Valore:** utilizzare il valore dell'identificazione personale salvato nel blocco note o nel file di testo menzionato nella sezione *Valore hash del certificato del plug-in.* È possibile immettere il valore della chiave anche dopo la creazione della chiave.

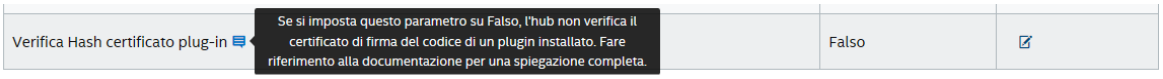
Fare clic su **Salva**. Per aggiornare i valori in un secondo momento, selezionare il collegamento **Modifica**. La nuova chiave viene visualizzata nella finestra Profilo.



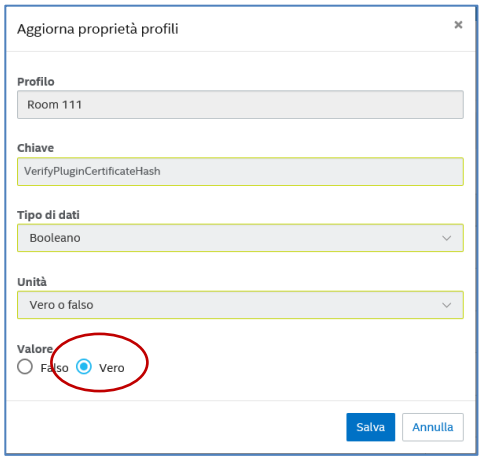
È necessario, inoltre, attivare la chiave **Verifica Hash certificato plug-in** impostandola su Vero. Il valore predefinito è Falso.



È possibile selezionare se si desidera attivare o disattivare il plug-in impostando su Vero o Falso o viceversa. Tenere presente che i valori della chiave garantiscono la validità del plug-in.



Fare clic sul collegamento Modifica per modificare il valore su **Vero** e quindi fare clic su **Salva**.



Le impostazioni del plug-in sono state attivate.

6 Installazione del client

6.1 Pre-Installation dei client

Il client deve essere in grado di individuare il server Enterprise ed eseguire l'archiviazione. Per eseguire l'archiviazione e comunicare con il server Enterprise, l'applicazione Intel Unite richiede di impostare un'esenzione nel firewall del client.
Quando si esegue il programma di installazione del client, vengono richiesti i dettagli della connessione al server e viene data la possibilità di saltare la ricerca manuale (denominata **Specifica il server** nel processo di installazione) e di utilizzare invece il recupero informazioni dal record del servizio DNS. Durante l'esecuzione del programma di installazione del client, viene modificato il file ServerConfig.xml.

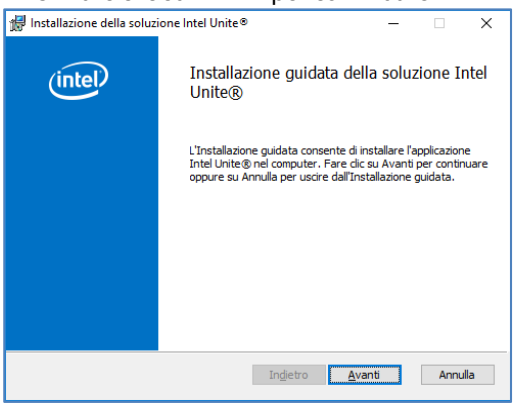
A seconda del metodo scelto per il blocco del PIN, è necessario sapere se utilizzare la selezione **Trova server automaticamente** o **Specifica il server** durante l'esecuzione dell'installazione.
Se si è certi dell'esistenza di un record del servizio DNS, è possibile selezionare **Trova server automaticamente**; è infatti preferibile utilizzare la ricerca automatica per evitare errori di digitazione. In caso di dubbio, utilizzare l'opzione **Specifica il server** (ricerca manuale), in cui è richiesto di conoscere il nome host per il server Enterprise.

Nota: se un server è definito nel file ServerConfig.xml, questo avrà precedenza sul record del servizio DNS.

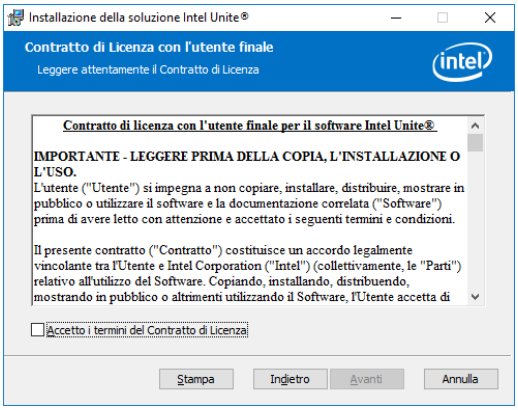
Dispositivi client mobili: tutti i dispositivi client devono essere connessi alla rete aziendale oppure utilizzare una VPN opportunamente configurata. Sono inclusi i dispositivi iOS e Android. I tablet e i telefoni, normalmente impiegati per uso personale, che non sono connessi alla rete aziendale ma a quella del proprio gestore potrebbero non essere in grado di connettersi a una sessione dell'app Intel Unite per via di un firewall aziendale che non consente queste connessioni. Per ulteriori informazioni, vedere la sezione Dispositivi client mobili.

6.2 Installazione di un client Windows

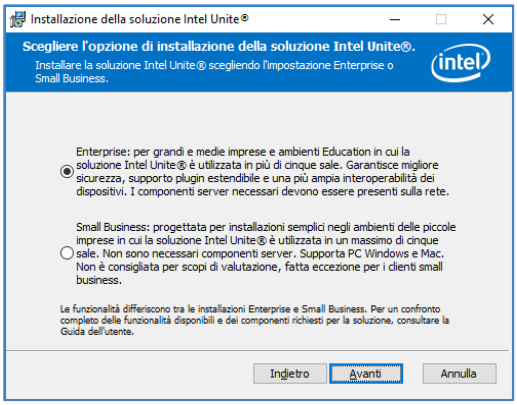
- Individuare la cartella del programma di installazione ed eseguire il file di installazione del client: **Intel Unite Client.mui.msi.** Fare clic su **Avanti** per continuare.



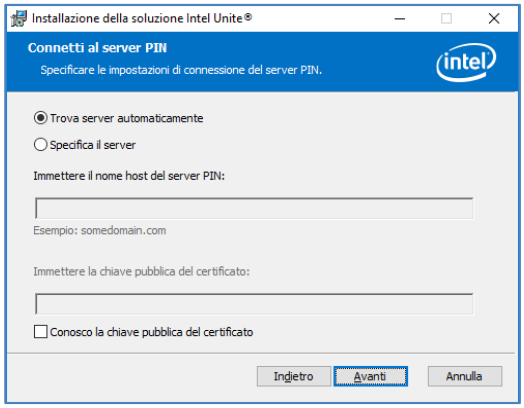
- Selezionare la casella **Accetto i termini del contratto di licenza** e quindi fare clic su **Avanti**.



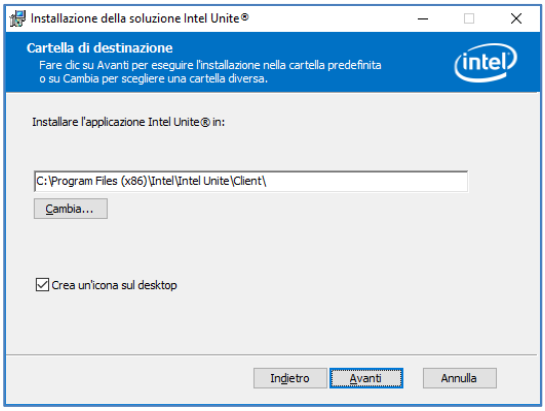
- Selezionare **Enterprise** e fare clic su **Avanti**



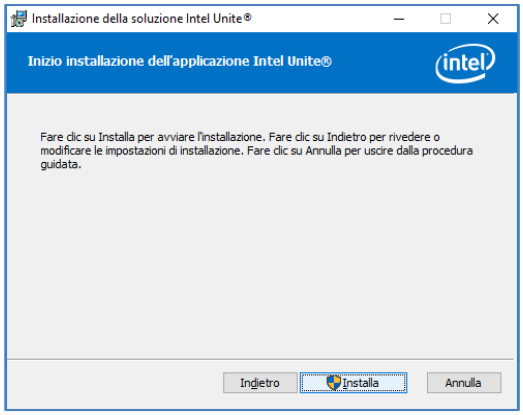
- In questa finestra specificare le impostazioni di connessione del server PIN. Le opzioni sono le seguenti:
  - **Trova server automaticamente**: si tratta dell'opzione più indicata (impostazione predefinita).
  - **Specifica il server**: in questo passaggio, è necessario conoscere il nome host per il server Enterprise.
    - **Immettere la chiave pubblica del certificato**: questa opzione può essere selezionata solo quando si sceglie **Specifica il server.**
    - Immettere la **chiave pubblica del certificato** se si è in possesso della chiave e se è stato selezionato questo metodo.
- Selezionare l'opzione e fare clic su **Avanti** per continuare.



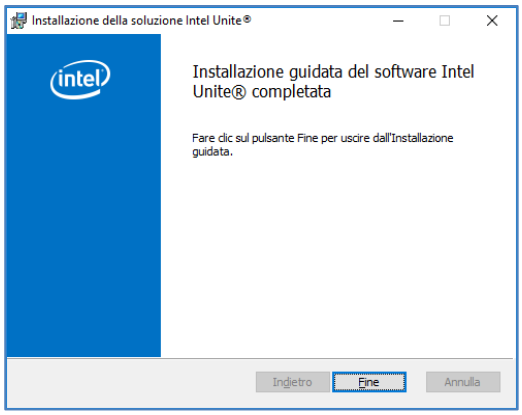
- La finestra **Cartella di destinazione** si apre con la cartella predefinita in cui risiederà il client nell'applicazione Intel Unite; se si desidera, è possibile modificare la cartella di destinazione, altrimenti mantenere la posizione predefinita.



- Per rivedere le impostazioni, è possibile tornare indietro oppure, per continuare, fare clic su **Installa**.



- Alla fine dell'installazione, viene visualizzata la finestra **Wizard di installazione del software Intel Unite® completato**. Fare quindi clic su **Fine.**

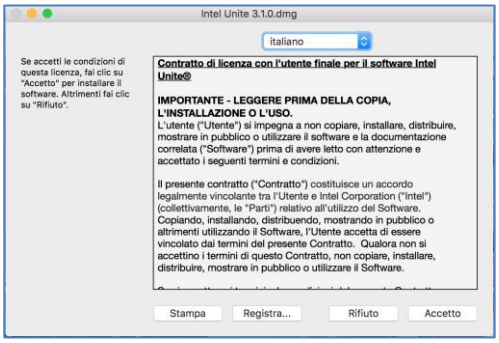


- Viene visualizzata la finestra **Connetti a uno schermo** illustrata di seguito:

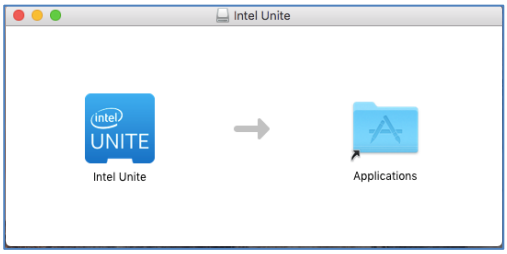
- Per connettersi all'hub, immettere il numero del PIN indicato sul monitor o sullo schermo. Per impostazione predefinita, il PIN cambia ogni cinque minuti.
- Per ulteriori informazioni sull'utente e sulle funzioni, consultare la **Guida dell'utente alla soluzione Intel Unite®.**

6.3 Installazione di un client macOS

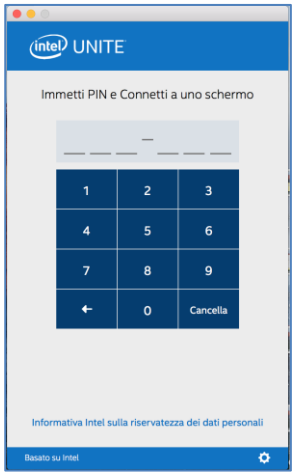
- Individuare il file **Intel Unite MacOS X,X.dmg** e scaricare il software sul client Mac. Fare doppio clic sul file per estrarre l'applicazione.
- Verrà richiesto di accettare un **Contratto di licenza con l'utente finale**. Fare clic su **Accetta** per continuare.



- Dopo l'estrazione, trascinarlo nella cartella Applicazioni.



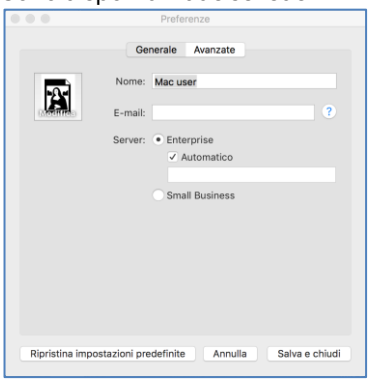
- Accedere a tale cartella e individuare l'applicazione; fare clic sul file per avviarlo.
- Si apre la schermata **Immetti PIN e connetti a uno schermo**; per connettersi all'hub, immettere il PIN indicato sul monitor o sullo schermo e avviare la condivisione.

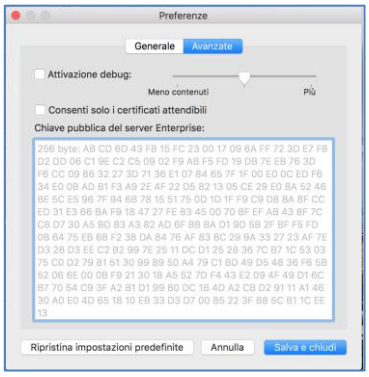


- Per ulteriori informazioni sull'utente e sulle funzioni, consultare la **Guida dell'utente alla soluzione Intel Unite®.**

Nota: l'applicazione utilizzerà il rilevamento automatico DNS (record di servizio DNS) per individuare il server Enterprise. In alternativa è possibile indicare un server Enterprise predefinito modificando le impostazioni di com.intel.Intel-Unite.plist, disponibile nella cartella ~/Library/Preferences dell'utente:

defaults write com.intel.Intel-Unite EnterpriseServer myServer.mydomain.myTLD . Per ulteriori informazioni, consultare la sezione *Soluzione Intel Unite per macOS* di questa guida.
È possibile, inoltre, modificare il server Enterprise al quale si connette l'applicazione. Fare clic sull'icona a forma di ingranaggio nell'angolo inferiore destro della finestra **Connetti schermo** per accedere alle **Impostazioni**.
Sono disponibili due schede:



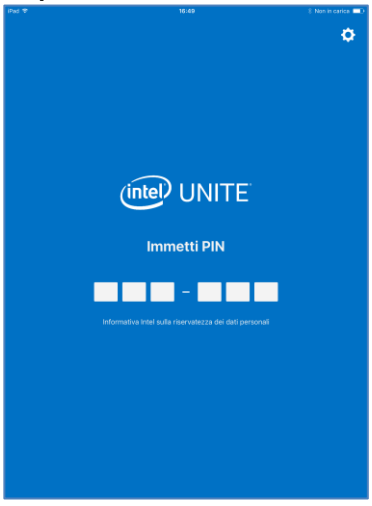


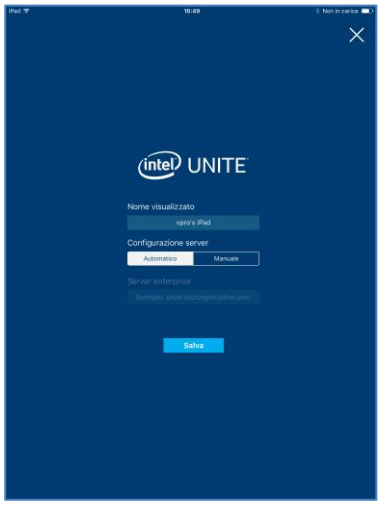
Generale: consente di immettere il nome, l'indirizzo e-mail e l'avatar dell'utente. Inoltre è possibile selezionare se la connessione tra questo computer client e il server Enterprise avverrà automaticamente (impostazione predefinita) o specificando un percorso definito del server.
Avanzate: tramite questa scheda è possibile selezionare l'opzione **Attiva debug** o scegliere se si desidera accettare solo **Certificati attendibili**.

6.4 Installazione di un client iOS

L'app è compatibile con tutti gli iPad eccetto l'iPad 2010 originale.

- Su client iOS (ad esempio, su iPad), andare all'Apple App Store e scaricare il software Intel Unite per il client.
- Alla fine del download, aprire l'app.
- Fare clic sull'icona a forma di ingranaggio nell'angolo superiore destro per accedere a **Impostazioni** e immettere le informazioni richieste.



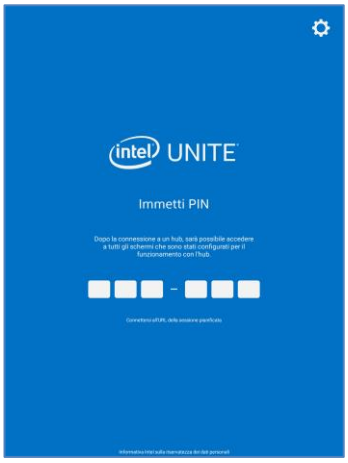


- Nelle **Impostazioni** inserire il Nome visualizzato e le informazioni sul Server.
- È possibile selezionare **Automatico** per trovare il server, oppure, se si desidera connettersi a un server specifico, fare clic su **Manuale** e inserire il server desiderato.
- Fare clic su **Salva**.

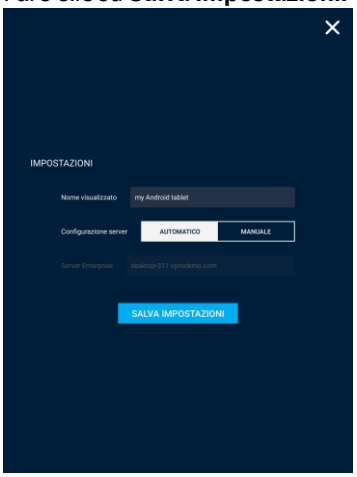
- Per connettersi all'hub, immettere il PIN indicato sul monitor o sullo schermo e avviare la condivisione.
- Per ulteriori informazioni sull'utente e sulle funzioni, consultare la **Guida dell'utente alla soluzione Intel Unite®.**

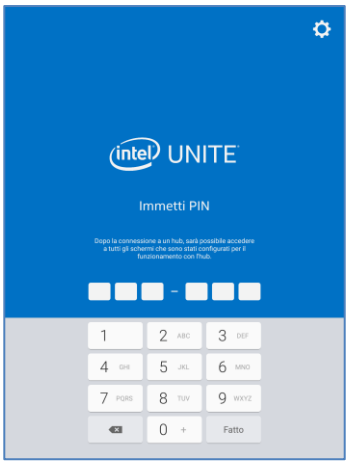
6.5 Installazione di un client Android

- Sul dispositivo Android, andare all'app store di Google e scaricare il software Intel Unite per il client.
- Alla fine del download, aprire l'app.
- Fare clic sull'icona a forma di ingranaggio nell'angolo superiore destro per accedere a **Impostazioni** e immettere le informazioni richieste.



- Nelle **Impostazioni** inserire il Nome visualizzato e le informazioni sul Server.
- È possibile selezionare **Automatico** per trovare il server, oppure, se si desidera connettersi a un server specifico, fare clic su **Manuale** e inserire il server desiderato.
- Fare clic su **Salva impostazioni.**

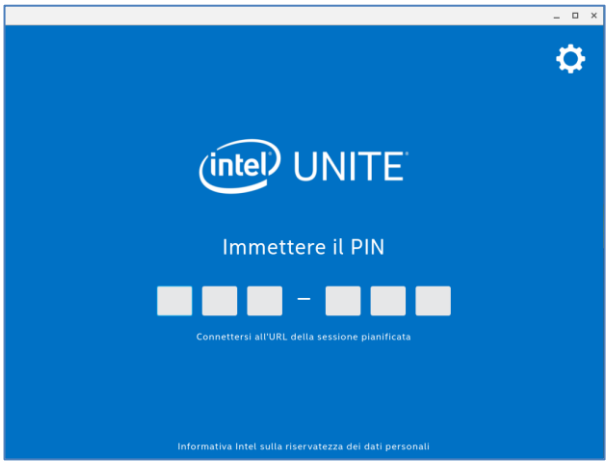




- Per connettersi all'hub, immettere il PIN indicato sul monitor o sullo schermo e avviare la condivisione.
- Per ulteriori informazioni sull'utente e sulle funzioni, consultare la **Guida dell'utente alla soluzione Intel Unite®.**

6.6 Installazione di un client Chrome OS

- Sul dispositivo Chromebook, andare all'app store di Google e scaricare il software Intel Unite per il client.
- Alla fine del download, aprire l'app.
- Fare clic sull'icona a forma di ingranaggio nell'angolo superiore destro per accedere a **Impostazioni** e immettere le informazioni richieste.



- Nelle Impostazioni inserire il Nome visualizzato, l'Indirizzo e-mail e le informazioni sul Server. È possibile selezionare **Automatico** per trovare il server, oppure, se si desidera connettersi a un server specifico, fare clic su **Manuale** e inserire il server desiderato.
- Fare clic su **Salva impostazioni.**

Per connettersi all'hub, immettere il PIN indicato sul monitor o sullo schermo e avviare la condivisione. Per ulteriori informazioni sull'utente e sulle funzioni, consultare la **Guida dell'utente alla soluzione Intel Unite®.**

6.7 Configurazione del client

Le impostazioni di configurazione del client possono essere modificate tramite il portale di amministrazione. Nel portale di amministrazione è presente un profilo predefinito con impostazioni di configurazione predefinite, applicate a tutti i client che eseguono l'archiviazione con il server. Quando viene stabilita una connessione dal client al server Enterprise, viene eseguito il push delle opzioni di configurazione nel client. Le impostazioni vengono aggiornate ogni volta che il client effettua l'archiviazione.
Per approfondire le opzioni di configurazione, consultare la Configurazione del profilo .

7 Installazione avanzata

7.1 Programmi di installazione con script

Questa sezione spiega come eseguire i programmi di installazione senza avvisare, ossia senza che vengano visualizzati menu o finestre. In questa modalità, i parametri delle proprietà vengono inviati al programma di installazione tramite una riga di comando.
Per eseguire i programmi di installazione senza avvisare, aprire il prompt dei comandi e utilizzare la seguente riga di comando:
msiexec /i "PERCORSO_FILE_MSI_CLIENT" PARAMETER=VALUE PARAMETER=VALUE ... /qn /l* "PERCORSO_DEL_LOG"

- Il valore /i contrassegna l'MSI specificato per l'installazione. "PATH_TO_CLIENT_MSI" è il nome del programma di installazione che si sta richiamando.
- "PARAMETER=VALUE PARAMETER=VALUE..." è un elenco dei parametri specificati nella tabella seguente.
- Il flag /qn esegue il programma di installazione in modalità non interattiva.
- Il contrassegno /l* registrerà l'output nel file di registro specificato.

NOTA: per visualizzare tutte le opzioni di **msiexec**, eseguire il comando: msiexec /?
Qui di seguito è riportato l'elenco completo dei parametri delle proprietà che possono essere inviati a ogni programma di installazione:

Parametri di installazione del server	Descrizione
DBHOSTNAME = "local" o "{IP}" o "{server},{port}" (l'impostazione predefinita è local)	Nome host di Microsoft SQL Server. In questa posizione il programma di installazione crea il database UniteServer e aggiunge l'account del servizio database. Se si installa il database sulla macchina corrente, non è necessario includere questo parametro, dal momento che l'impostazione predefinita è la posizione locale.
DBLOGONTYPE = "WinAccount" o "SqlAccount" → il valore predefinito è WinAccount	Consente di specificare il tipo di accesso per Microsoft SQL Server. Le opzioni disponibili sono l'autenticazione Windows o l'autenticazione SQL.
DBUSER = "{nome utente SQL}" DBPASSWORD = "{password SQL}"	Se il tipo di accesso è "SqlAccount", fornire il nome utente e la password. NOTA: l'account deve disporre delle autorizzazioni necessarie per aggiungere il database e creare l'account del servizio database.
DBLOGONPASSWORD = “{service account password}”	Si tratta della password che deve essere utilizzata dall'account del servizio per connettersi al database UniteServer.
DBLOGONPASSWORDCONF = “{service account password}”	Questa variabile deve avere lo stesso valore specificato in DBLOGONPASSWORD
Parametri per la selezione delle funzionalità del server	**Descrizione**

ADDLOCAL = "ALL"	Sono disponibili solo due opzioni: ALL = installare il database E il server PIN, il portale di amministrazione e la pagina di download. (non specificare questa variabile) = installare il server PIN, il portale di amministrazione e la pagina di download.
Parametri di installazione del client e dell'hub	**Descrizione**
PINSERVERLOOKUPTYPE = “Lookup” o “Manual” il valore predefinito è Lookup	Specifica in che modo l'applicazione individua il server PIN. L'opzione "Lookup" utilizza il record del servizio DNS, mentre l'opzione "Manual" richiede l'immissione dei parametri PINSERVER.
PINSERVER = "{nomehost}"	Si tratta del nome host del server a cui connettersi.
CERTKEYCHECKED = “1” o “0” Impostazione predefinita: 0	Parametro facoltativo. 0 = non verificare l'hashing della chiave del certificato 1= verificare l'hashing della chiave del certificato; è necessario specificare anche CERTKEY.
CERTKEY = "{chiave certificato}"	Parametro facoltativo. Immettere la chiave pubblica del certificato del server PIN.
COLLEGAMENTI	Facoltativo. Impostare su "1" per collocare le icone di scelta rapida sul desktop.
INSTALLTYPE = due valori possibili: "Enterprise" e "StandAlone".	Se INSTALLTYPE è "Enterprise", il client o l'hub verrà installato nella versione Enterprise. Se INSTALLTYPE è "StandAlone", il client o l'hub verrà installato nella versione Standalone.
SKIP_EXTENDED_DISPLAY= "1" o "0" Impostazione predefinita: 0	0 = Falso 1 = Vero

7.2 Chiavi di registro

Le chiavi di registro vengono scritte nel registro quando si eseguono i programmi di installazione e l'applicazione. I valori di alcune chiavi possono essere rettificati in base al risultato auspicato. Per conoscere le chiavi scritte dall'applicazione Intel Unite, consultare l'elenco riportato di seguito:

Chiavi di registro: (utente corrente)	Valore	Dispositivo
HKEY_CURRENT_USER\software\Intel\Unite\ ActiveConnection (DWORD)	[0 = nessun utente connesso 1= utente connesso]	Hub

HKEY_CURRENT_USER\software\Intel\Unite\ PublicKey (stringa)	[chiave pubblica del certificato di connessione]	Entra mbe
HKEY_CURRENT_USER\software\Intel\Unite\ CurrentPin (stringa)	[PIN corrente del sistema in uso]	Hub
HKEY_CURRENT_USER\software\Intel\Unite\ DoNotShowPrivacyStatement (DWORD)	[0 = mostra l'informativa sulla privacy all'avvio 1 = non mostra l'informativa sulla privacy]	Entra mbe
HKEY_CURRENT_USER\software\Intel\Unite\ HWThumbprint (stringa)	[hash di HW]	Entra mbe
HKEY_CURRENT_USER\software\Intel\Unite\ ServicePort (DWORD)	[porta su cui rimane in ascolto il servizio]	Hub
HKEY_CURRENT_USER\software\Intel\Unite\ ActivePresenter	[1 = il client sta effettuando la presentazione 0 = nessun client sta effettuando una presentazione]	Hub
HKEY_CURRENT_USER\software\Intel\Unite\PinPadWindows (DWORD)	[1 = l'applicazione è pronta per l'inserimento di un PIN 0 = negli altri casi]	Client
HKEY_CURRENT_USER\software\Intel\Unite\GuestAccess\SSID Riferimento: Guida al plug-in di ACCESSO GUEST	L'impostazione di un valore predefinito riduce il livello di sicurezza nell'accesso guest	Hub
HKEY_CURRENT_USER\software\Intel\Unite\GuestAccess\PSK Riferimento: Guida al plug-in di ACCESSO GUEST	L'impostazione di un valore predefinito riduce il livello di sicurezza nell'accesso guest	Hub

HKEY_CURRENT_USER\software\Intel\Unite\GuestAccess\Download Riferimento: Guida al plug-in di ACCESSO GUEST	Il collegamento predefinito per il download è http://192.168.173.1/download	Hub
HKEY_CURRENT_USER\software\Intel\Unite\ShowAvToggle (DWORD) = 1 (Interruttore Attiva/disattiva modalità A/V)	Modalità Aero Win7. Consente all'utente di alternare le modalità RTF e WebRTC.	Client
Chiavi di registro (sistema):	**Valore**	**Dispositivo**
HKEY_LOCAL_MACHINE\software\Intel\Unite\ HubUnlockPassword (stringa)	[password per uscire dall'applicazione hub]	Hub
HKEY_LOCAL_MACHINE\software\Intel\Unite\ DisableCheckCertificateChain (DWORD)	[set per certificati autofirmati, dove 1 = non controllare la catena di certificati di Enterprise (certificato del server)]	Entrambe
HKEY_LOCAL_MACHINE\software\Intel\Unite\ DisableUsageCollection (DWORD)	[1 = blocca la raccolta di tutti i dati di telemetria]	Entrambe
HKEY_LOCAL_MACHINE\software\Intel\Unite\WindowedMode (DWORD) (funziona solo in modalità Small Business, non in modalità Enterprise)	[1 = l'utente desidera l'avvio dell'hub in modalità finestra (con pulsanti per ridurre al minimo, ingrandire al massimo e uscire) 0 = negli altri casi]	Hub

HKEY_LOCAL_MACHINE\software\Intel\Unite\AllowInsecureCertificates (DWORD)	[1 = il controllo dell'algoritmo del certificato deve essere ignorato 0 = viene forzato l'uso di un certificato SHA2 da parte del certificato Enterprise]	Entrambe
HKEY_LOCAL_MACHINE\software\Intel\Unite\ShowOnlyInOneMonitor (DWORD)	[Questa chiave funziona solo se la modalità finestra è impostata su 1. 1 = verrà visualizzata una sola finestra PIN anche se sono collegati più monitor]	Hub
HKEY_LOCAL_MACHINE\SOFTWARE\Intel\Unite\S4BPlugin Keywords (stringa) = elenco,di,parole chiave,separate da virgola	Chiave utilizzata per il plug-in di Skype for Business	Hub
HKEY_LOCAL_MACHINE\software\Intel\Unite\ LogFile (stringa)	[percorso del file con accesso in scrittura per registrare i messaggi di debug in fase di esecuzione]	Entrambe

8 Guida al portale di amministrazione

Il portale di amministrazione è il portale Web per gli amministratori dell'applicazione Intel Unite, che consente di visualizzare e gestire i dispositivi sui quali è installata l'applicazione Intel Unite. Si tratta di uno dei componenti installati sul server Enterprise, insieme al servizio PIN e al server Web, durante la fase di installazione. Consultare la sezione sull'Installazione del server Enterprise. Il portale di amministrazione non deve trovarsi necessariamente sullo stesso server del database, a condizione che possa accedere a quest'ultimo.

Oltre all'aggiunta di nuove funzioni, anche l'aspetto del portale di amministrazione è cambiato: sono stati introdotti alcuni menu guida e informazioni sulle funzioni che semplificano la configurazione dei dispositivi client e degli hub.

- Per accedere al portale di amministrazione, aprire il browser e andare al collegamento assegnato al portale, ossia https://<nomeserver>/admin, dove <nomeserver> è il nome assegnato al server Intel Unite (nome predefinito = UniteServer, cioè https://uniteserver/admin)

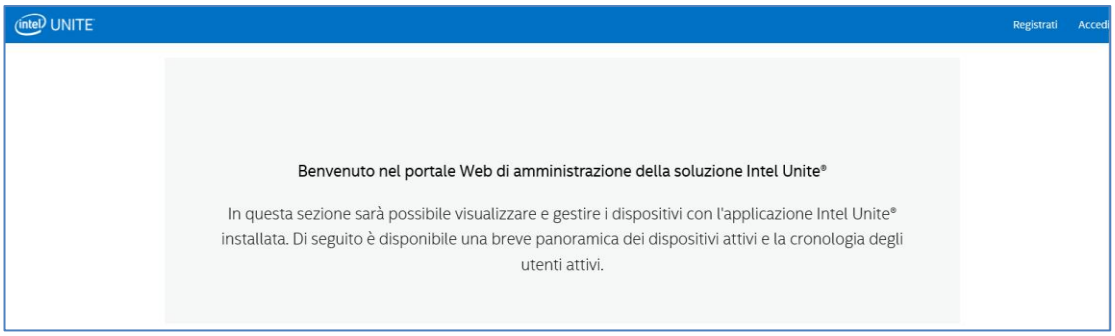
Quando l'amministratore IT esegue i programmi di installazione del software, viene creato un account amministratore predefinito con il nome utente e la password indicati di seguito:

- Utente: admin@server.com
- Password: Admin@1

Tale account dispone di accesso completo al portale di amministrazione e consente di eseguire l'accesso; il sistema, tuttavia, richiederà all'utente di modificarlo. Se si è già registrato un account, immettere le informazioni di accesso per accedere al portale di amministrazione.

8.1 Pagina di benvenuto del portale di amministrazione

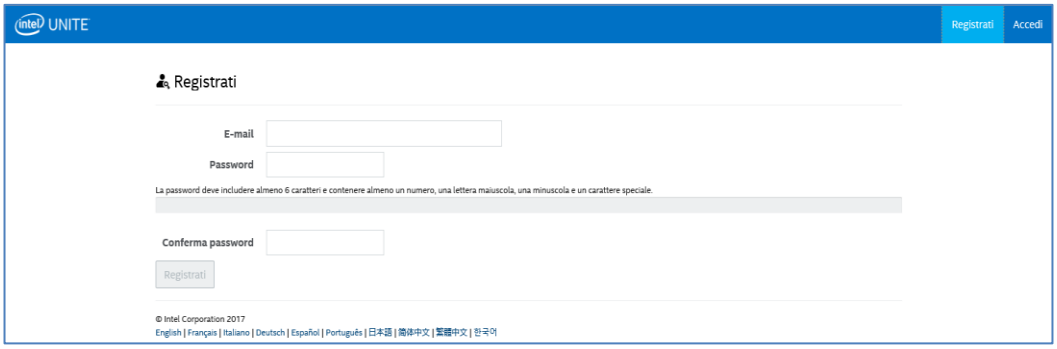
La pagina di benvenuto si apre non appena ci si connette al portale di amministrazione. Per accedere alla home page, è necessario eseguire l'accesso con l'account predefinito creato durante il processo di installazione o con le informazioni del proprio account.



8.1.1 Registrare un account

Per registrare un account, verificare di essersi disconnessi dal portale di amministrazione.

- Fare clic sul collegamento **Registrati** in alto a destra nella barra di navigazione.
- Specificare nel modulo l'indirizzo e-mail e la password desiderati, quindi fare clic su **Registrati**.



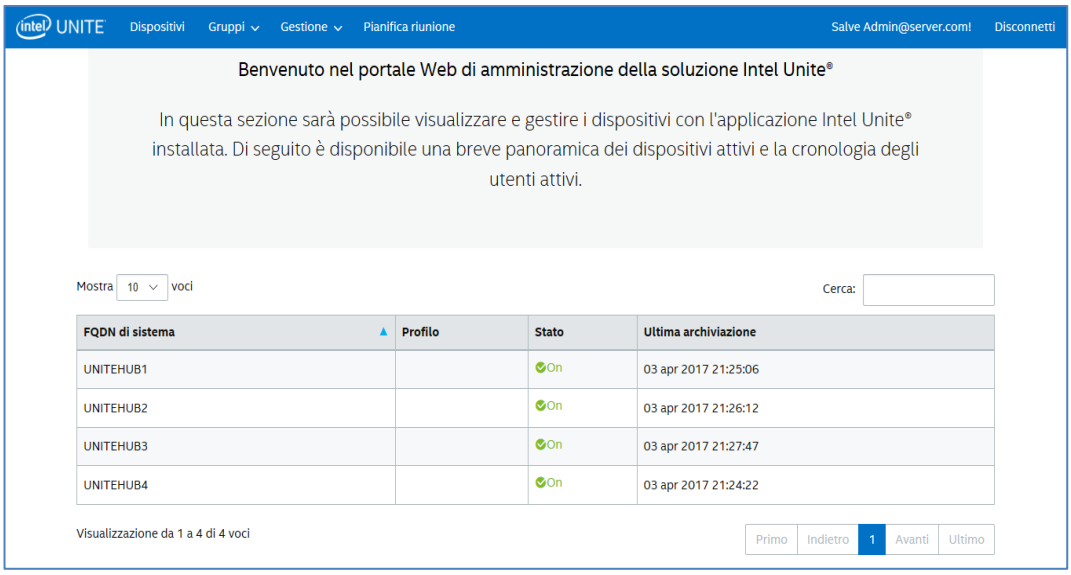
- In alternativa, è possibile aggiungere/registrare gli utenti tramite la scheda Gestione dopo aver effettuato l'accesso al portale di amministrazione.

8.1.2 Accesso con un account esistente

È possibile accedere con un account registrato o utilizzare l'account predefinito creato durante l'installazione. Tenere presente, tuttavia, che tale account dispone di accesso completo al portale di amministrazione ed è pertanto consigliabile modificare la password per limitare gli accessi al portale.

8.2 Home page del portale di amministrazione

Questa pagina contiene un messaggio di benvenuto e fornisce una rapida panoramica di tutti i sistemi attivi, ossia client e hub, che hanno eseguito l'archiviazione con il server. Nella tabella sono indicati il nome di ogni **Sistema**, il **Profilo** assegnato a ciascuno di essi, lo stato **ON** o **OFF**, la data e l'ora dell'**ultima archiviazione**.



Queste voci possono essere filtrate usando la casella di ricerca con più parole chiave; ogni parola chiave eseguirà la ricerca in tutte le colonne. Per selezionare il numero di voci da visualizzare in questa finestra, fare clic sul pulsante Mostra <numero> voci. È possibile visualizzare 10, 25, 50 o un massimo di 100 voci.

8.2.1 Barra di navigazione

La barra di navigazione indirizza l'utente nelle diverse aree del portale Web; mostra il nome dell'utente attualmente connesso oppure, se nessun utente ha eseguito l'accesso, riporta la dicitura **Registrati**.

Le pagine e le sottopagine del portale Web sono le seguenti:

- **Dispositivi**
- **Gruppi**
  - Gruppo di dispositivi
  - Profili
- **Gestione**
  - Proprietà del server
  - Utenti
  - Ruoli
  - Moderatori
  - PIN riservato
  - Telemetria
- **Pianifica riunione**

Per ulteriori informazioni, consultare la sezione assegnata a ogni argomento in questo capitolo del portale di amministrazione.

8.2.2 Nomenclatura collegamenti/icone

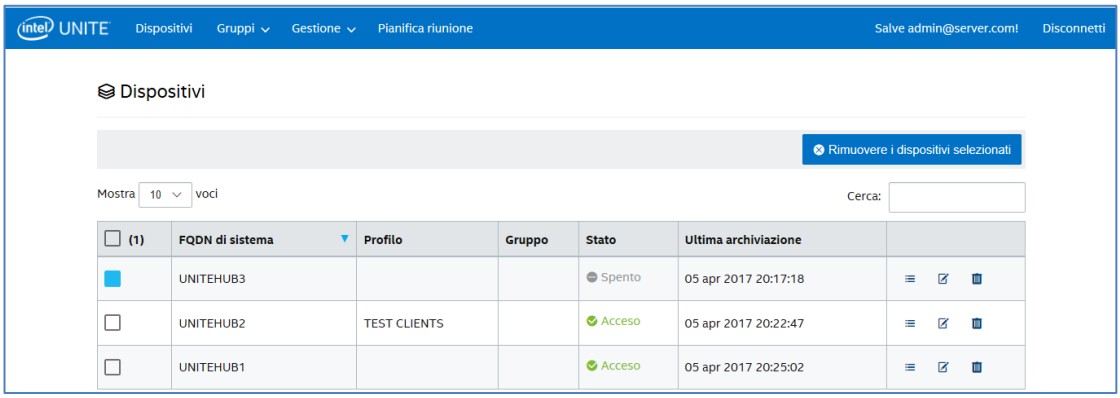
Nel portale di amministrazione sono sempre disponibili i collegamenti o le icone indicati di seguito:

	Modifica
	Visualizza dettagli
	Visualizza dispositivi
	Elimina
	Finestra di dialogo contenente le informazioni di un valore specifico

Posizionando il cursore sopra l'icona, è possibile visualizzare le informazioni relative all'elemento.

8.3 Pagina Dispositivi

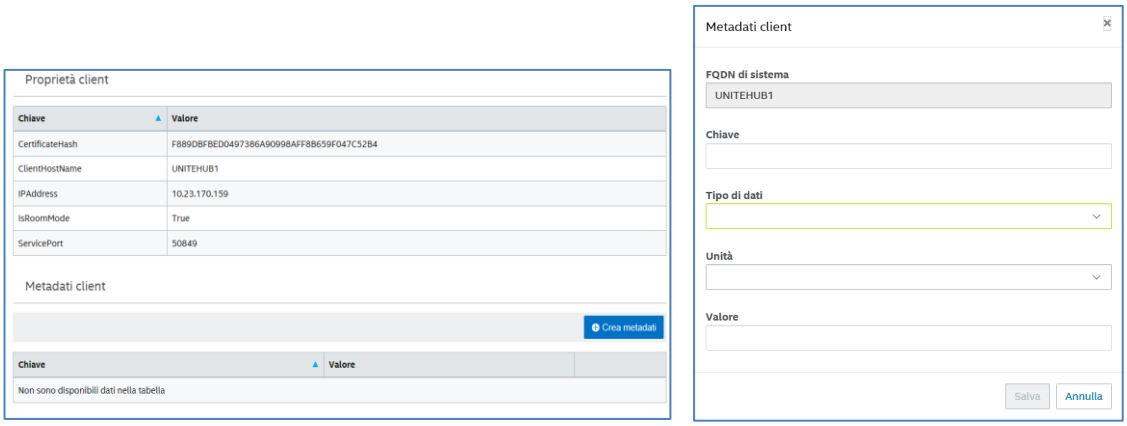
La pagina Dispositivi contiene tutti i dispositivi attualmente presenti nel database. È possibile selezionare un dispositivo specifico e fare clic su **Visualizza**, **Modifica**, **Aggiorna** o **Rimuovi** in base alle esigenze.



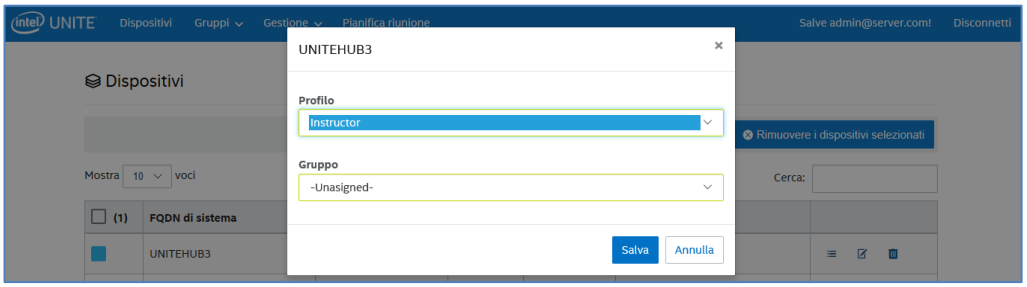
Nella pagina **Dispositivi** è disponibile quanto segue:

- **FQDN di sistema** è il nome di dominio completo del client/hub
- **Profilo** contiene impostazioni di configurazione applicate al dispositivo
- **Gruppo** è il nome del gruppo al quale è stato assegnato un dispositivo
- **Stato** mostra se il dispositivo è attivo - ON (verde) - o inattivo - OFF (grigio) -
- **Ultima archiviazione** è la data e l'ora dell'ultima archiviazione svolta dal dispositivo con il server
- **Dettagli**: facendo clic sul collegamento **Visualizza dettagli**, si apre la finestra **Proprietà client** con le proprietà del sistema e i relativi metadati. Alcuni dei tasti nella sezione **Proprietà client** sono i seguenti:
    - CertificateHash
    - ClientHostName
    - IPAddress
    - IsRoomMode
    - SevicePort

  Per ulteriori informazioni sui valori validi per ogni chiave, consultare la sezione Configurazione del profilo che descrive in dettaglio le chiavi e i valori corrispondenti.



Collegamento **Modifica**: facendo clic sul collegamento Modifica, è possibile modificare il profilo del dispositivo e assegnarlo a un gruppo specifico



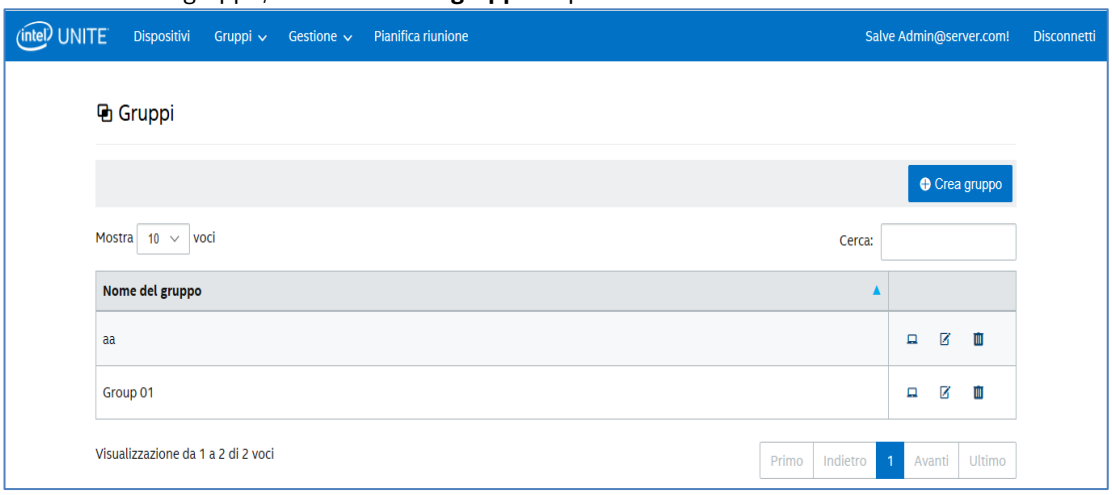
Collegamento **Elimina**: facendo clic sul collegamento Elimina, è possibile rimuovere il dispositivo dal portale di amministrazione. Prima della rimozione viene visualizzato un messaggio di conferma. In alternativa è possibile selezionare uno o più dispositivi nella colonna sinistra e fare clic sul pulsante **Rimuovere i dispositivi selezionati.**

8.4 Pagina Gruppi

La pagina **Gruppi** prevede un menu con due opzioni: **Gruppo di dispositivi** e **Profili**.

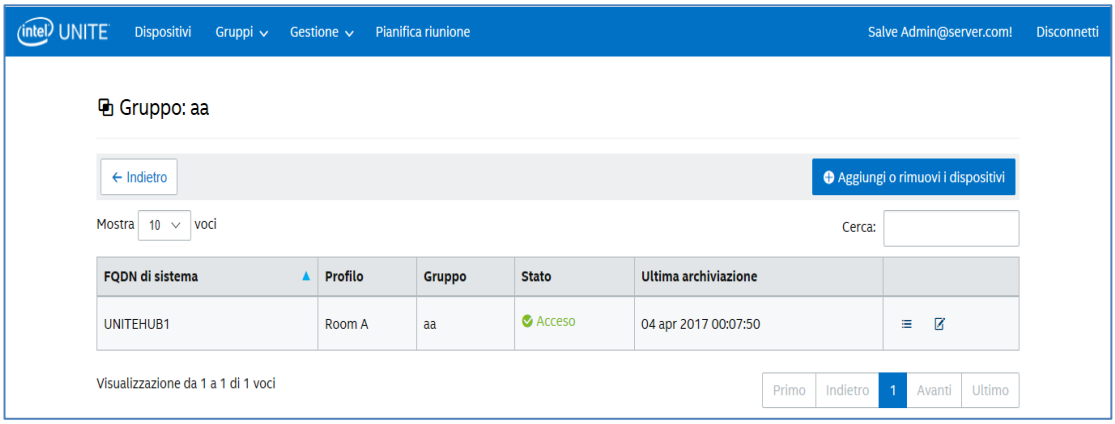
8.4.1 Gruppi > Gruppo di dispositivi

Gruppi di dispositivi serve per raggruppare i dispositivi a scopo di monitoraggio, funzionalità o comodità. I dispositivi possono essere associati allo stesso profilo o a un profilo diverso assegnato a un gruppo. In questa pagina è possibile creare, visualizzare, modificare ed eliminare i gruppi e le voci di ciascuno. Per creare un nuovo gruppo, fare clic su **Crea gruppo** e specificare un nome.



Dopo aver creato il gruppo, è possibile:

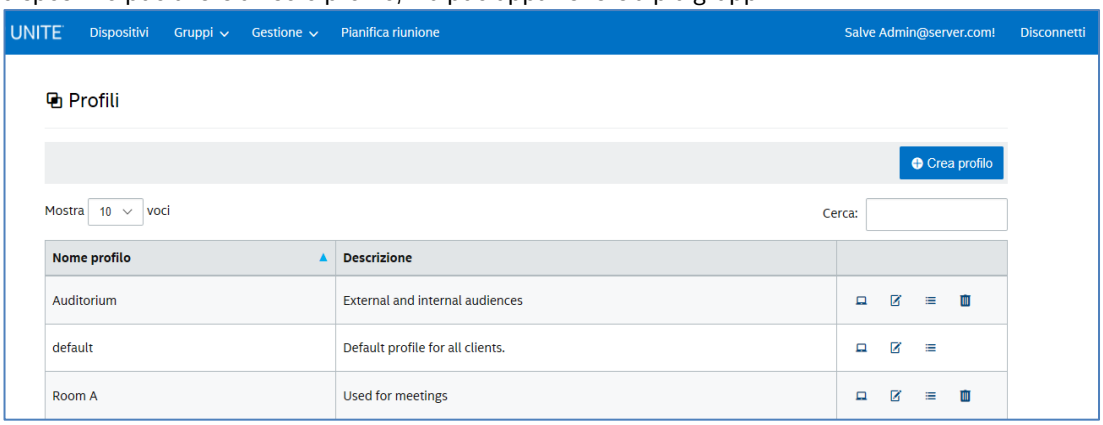
- Fare clic sul collegamento **Visualizza dispositivi** per aggiungere o rimuovere i dispositivi dal gruppo selezionato oppure fare clic sul collegamento **Dettagli**, nella colonna destra, per visualizzare le proprietà e i metadati di ogni sistema appartenente a questo gruppo.



- Fare clic sul collegamento **Modifica** per aggiornare o modificare il **Nome gruppo**.
- Se sono state apportate delle modifiche, fare clic su **Salva** per salvarle.

8.4.2 Gruppi > Profili

Questa pagina permette di creare, visualizzare, eliminare e modificare i profili. Presenta un layout e un funzionamento simili a quelli dell'opzione **Gruppo di dispositivi**, ma contiene i profili. La differenza tra **Profili** e **Gruppi** consiste nel fatto che Profili contiene le opzioni di configurazione per i dispositivi. Ogni dispositivo può avere un solo profilo, ma può appartenere a più gruppi.



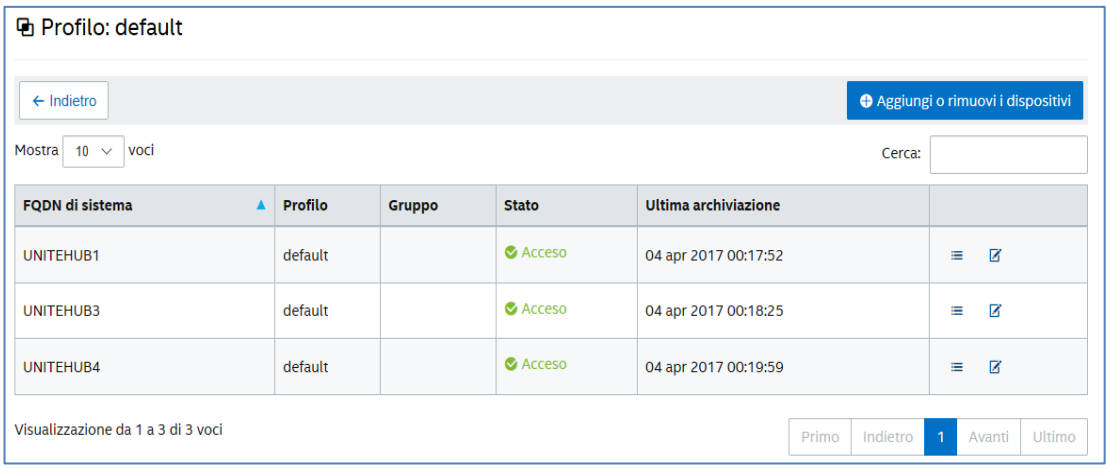
La pagina **Profili** mostra il **Nome profilo** e la **Descrizione** di ogni profilo disponibile nel server. I profili sono applicati a tutti i dispositivi che eseguono l'archiviazione con il server Enterprise. Il profilo **predefinito** non può essere eliminato nel portale di amministrazione.

Se si fa clic sul collegamento **Visualizza dispositivi**, è possibile visualizzare i sistemi assegnati al profilo selezionato.
Se si fa clic sul collegamento **Modifica**, è possibile aggiornare il nome del profilo e la sua descrizione.

Se si fa clic sul collegamento **Visualizza dettagli** di un profilo specifico, è possibile accedere e modificare le impostazioni dei valori e delle chiavi del profilo predefinito o creato di recente. L'elenco visualizzato mostra ogni chiave, il valore corrispondente e il collegamento **Modifica** per aggiornare o personalizzare in base alle esigenze. Per informazioni dettagliate sulle chiavi e sui valori corrispondenti, consultare la sezione *Configurazione del profilo*.

8.4.2.1 Profilo predefinito

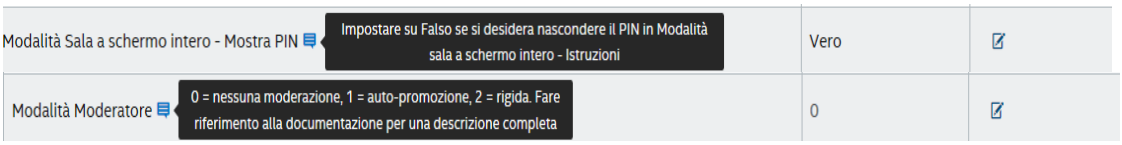
Il profilo **predefinito** non può essere eliminato nel portale di amministrazione. È tuttavia possibile creare altri profili sapendo che quello predefinito non verrà eliminato.



Valori e chiavi **predefiniti**:

Chiave	Valore	
Consenti trasferimento file	Falso	
Supporto streaming audio/video	Vero	
Modifica il PIN durante la riunione	Vero	
Disattiva visualizzazione remota	Falso	
Visualizza dimensioni PIN	48	
Visualizza trasparenza PIN	100	
Estensioni di file bloccate		
Dimensioni massime dei file	2147483647	
Modalità Sala a schermo intero	Vero	
Modalità Sala a schermo intero - Colore sfondo		
Modalità Sala a schermo intero - Estensione immagine di sfondo	Falso	
Modalità Sala a schermo intero - URL sfondo		
Modalità Sala a schermo intero - Istruzioni	{pin}	
Modalità Sala a schermo intero - Colore PIN		
Modalità Sala a schermo intero - Mostra PIN	Vero	
Modalità Sala a schermo intero - Colore testo		
Modalità Sala a schermo intero - Carattere testo		
Hub - Blocca tastiera	Falso	
Hub - Mostra orologio	Vero	
Modalità Moderatore	0	
Indirizzo e-mail per l'invio degli errori		
Porta di ascolto servizio	0	
Compressione riquadri	85	
Dimensione riquadri	128	
Verifica Hash certificato plug-in	Vero	

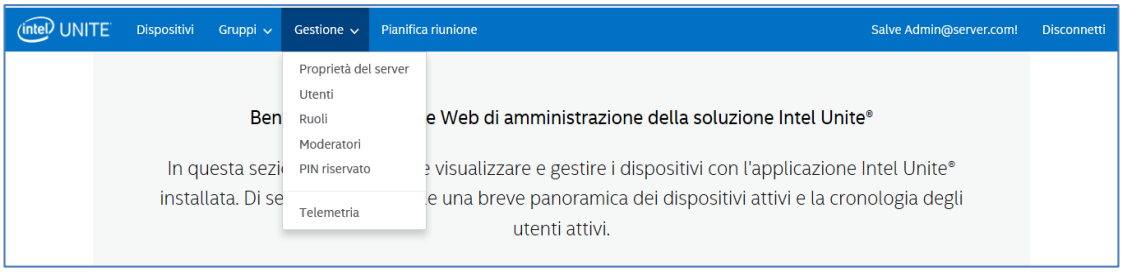
Accanto a ogni chiave è disponibile una finestra di dialogo. Se si posiziona il cursore del mouse su tale finestra, è possibile visualizzare i valori e/o le informazioni di ogni chiave. Questi dati sono utili da consultare prima di procedere alla modifica della chiave. Vedere i due esempi riportati di seguito:



Per informazioni dettagliate sulle chiavi e sui valori corrispondenti, consultare la tabella nella sezione Configurazione del profilo.

8.5 Pagina Gestione

La pagina Gestione include numerose pagine secondarie:

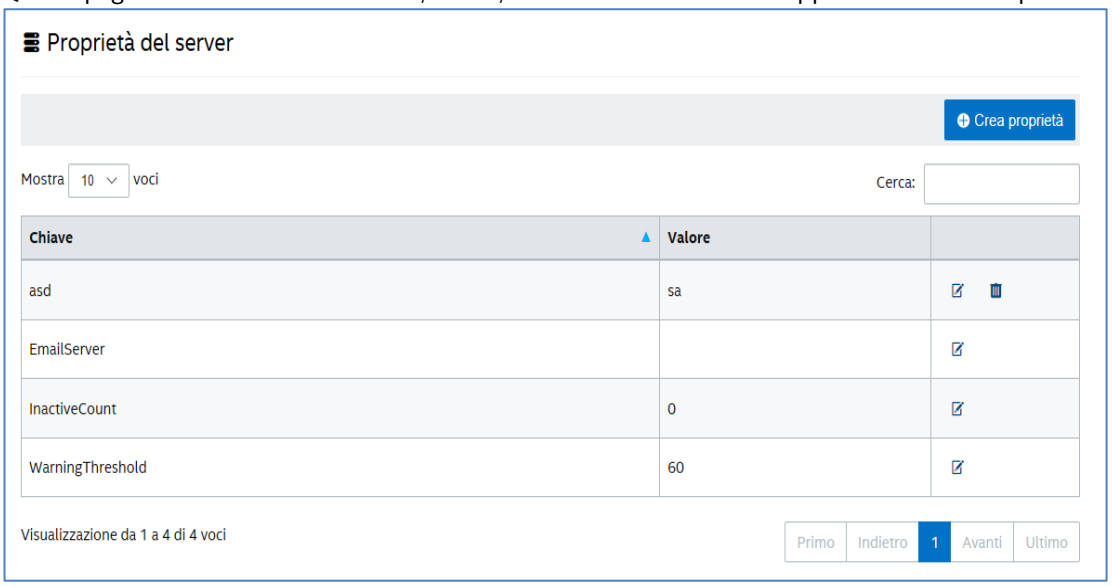


- **Proprietà del server**: l'interfaccia per la visualizzazione e la modifica delle chiavi e dei valori del server.
- **Utenti**: è possibile aggiungere, rimuovere o modificare manualmente qualsiasi account in questa pagina.
- **Ruoli**: consente di creare nuovi ruoli, aggiornare quelli esistenti, assegnare utenti ai ruoli e modificare le autorizzazioni per la gestione degli utenti.
- **Moderatori**: questa funzione consente agli utenti di assumere il controllo di una riunione raggruppando le funzionalità in ruoli. In questa sezione è possibile aggiungere o rimuovere facilmente i moderatori.
- **PIN riservato**: questa funzione consente agli amministratori IT di assegnare PIN a determinate sale. I PIN possono essere generati in modo automatico o impostati manualmente dal reparto IT in base alla posizione della sala o ai requisiti della sessione che si terrà.
- **Telemetria**: per poter visualizzare i dati di telemetria, è necessario installare il plug-in di telemetria per la soluzione Intel Unite®. Il plug-in di telemetria consente agli amministratori IT di raccogliere le informazioni sull'utilizzo dell'applicazione Intel Unite e dei dispositivi client collegati a ciascun hub.

Per ulteriori informazioni sulle pagine secondarie, vedere le sezioni di seguito.

8.5.1 Gestione > Proprietà del server

Questa pagina consente di visualizzare, creare, modificare ed eliminare coppie di valori chiave per i server.



Le chiavi utilizzate dal portale di amministrazione sono le seguenti:

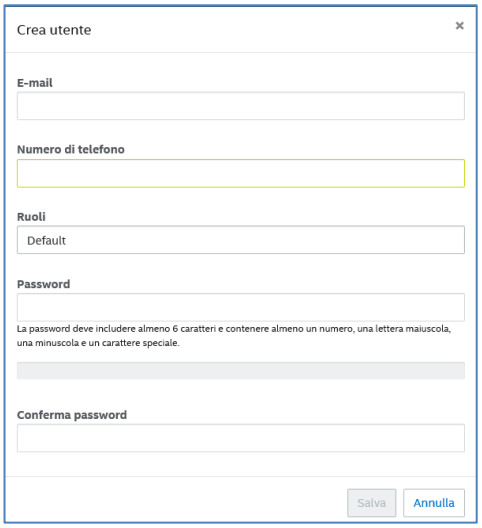
- **EmailServer**: questo è l'indirizzo e-mail al quale il server invierà le notifiche.
- **InactiveCount:** opzione usata dallo strumento di monitoraggio dello stato dell'applicazione Intel Unite che invia i messaggi e-mail agli utenti cui è stato assegnato il ruolo Notifiche.
- **WarningThreshold**: utilizzato per specificare la soglia in minuti che determina quando un dispositivo deve essere considerato inattivo, con un valore predefinito di 60 minuti.

Se si fa clic sul collegamento **Modifica**, è possibile aggiornare le chiavi in base alle esigenze.

8.5.2 Gestione > Utenti

La pagina **Utenti** mostra un elenco di tutti gli utenti registrati sul portale di amministrazione, informazioni sull'eventuale blocco dell'account e i loro ruoli. Per aggiornare queste informazioni, è anche possibile fare clic sul collegamento **Modifica**.

Per aggiungere un nuovo utente, fare clic su **Crea utente** e specificare un indirizzo e-mail, un numero di telefono e una password. Durante la creazione dell'utente, è inoltre possibile assegnare un ruolo specifico o lasciare il valore predefinito. Per assegnare i diritti di accesso al nuovo utente, è possibile definire alcuni ruoli e assegnare l'utente a uno di essi.



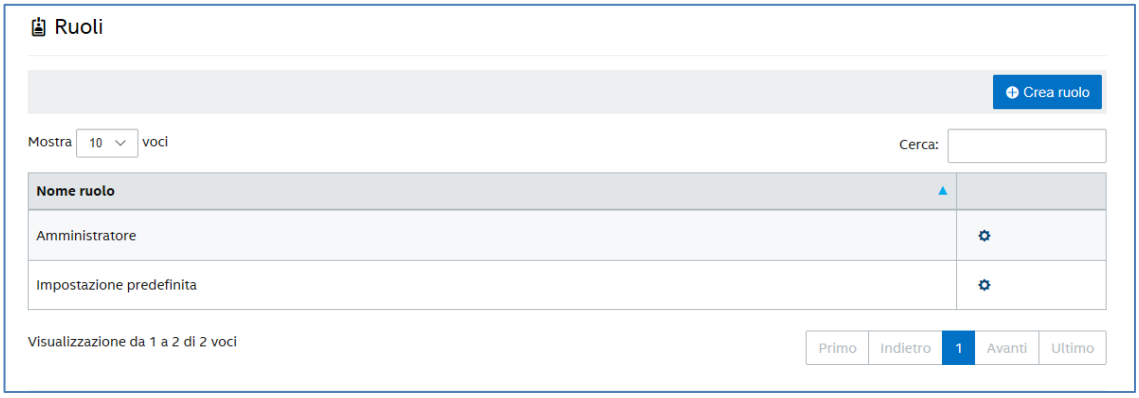
In questa stessa pagina, se si fa clic sul ruolo stesso (**Predefinito** o **Amministratore**), viene visualizzata la pagina **Ruoli**. Continuare con la sezione successiva per ottenere ulteriori informazioni sui **Ruoli**.

NOTA sull'account predefinito: quando si aggiunge un nuovo account utente eseguendo l'accesso con le credenziali predefinite admin@server.com, il messaggio e-mail di verifica non viene inviato

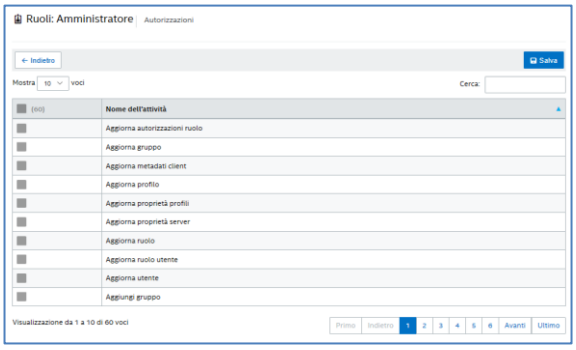
automaticamente. Per verificare manualmente l'indirizzo e-mail, effettuare l'accesso con il nuovo account, fare clic su "Salve <nome utente>!" in alto a destra nella barra di navigazione, quindi fare clic sul pulsante "**Invia verifica tramite e-mail**" nella parte inferiore della pagina. Prima di questa operazione, è necessario modificare le impostazioni di posta elettronica del server nel file web.config xml. Consultare la sezione sulle Impostazioni del server di posta elettronica.

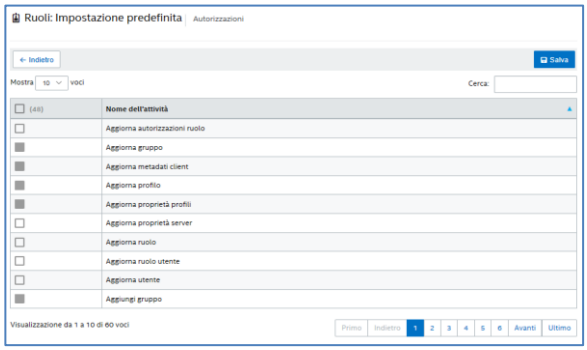
8.5.3 Gestione > Ruoli

Questa pagina mostra i ruoli attualmente definiti, ossia **Amministratore** e **Predefinito**. È possibile aggiungere nuovi ruoli e modificare i ruoli correnti. Di per sé, i ruoli non regolano l'accesso al portale, ma le azioni sul portale (ad esempio, la creazione di un utente) sono limitate a determinati ruoli, che sono associati a un set di utenti.



Per visualizzare le attività e le autorizzazioni assegnate a ogni ruolo, fare clic sull'icona a forma di ingranaggio nella colonna destra. Viene visualizzata la finestra **Autorizzazioni**. Le attività assegnate possono essere personalizzate per consentirne l'esecuzione da parte di un determinato gruppo di ruoli.





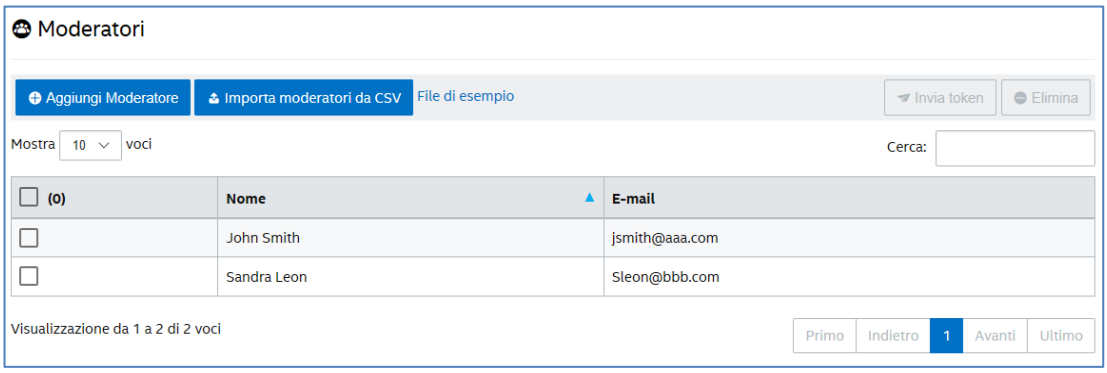
Per aggiungere un nuovo ruolo, fare clic sul pulsante **Crea ruolo** e modificare il nome corrispondente. Quindi, nella pagina **Ruoli**, fare clic sull'icona a forma di ingranaggio e selezionare le attività che il ruolo dovrà svolgere. L'opzione permette di aggiungere o rimuovere le autorizzazioni.
Tenere presente che è possibile assegnare più ruoli agli utenti.

8.5.4 Gestione > Moderatori

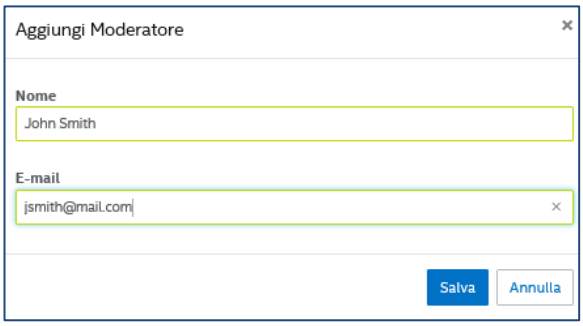
Questa pagina mostra gli utenti a cui è stato assegnato il ruolo di Moderatore. Per designare un utente come Moderatore, è necessario completare alcuni passaggi.

Si possono aggiungere i Moderatori in due modi: è possibile fare clic su **Aggiungi moderatore** e compilare con i dati richiesti; oppure è possibile fare clic su **Importa moderatori da CSV** per importare un file CSV con i nomi e gli indirizzi e-mail corrispondenti da aggiungere all'elenco. Se si sceglie di importare un file CSV con i nomi dei Moderatori, verificare sia rispettato il seguente formato: **Nome, Indirizzo e-mail, Azione**. In alternativa, fare clic su **File di esempio** per visualizzare il formato valido.

Esempio: John Smith,jsmith@aaa.com,Aggiungi
Sandra Leon,sleon@bbb.com,Cancella

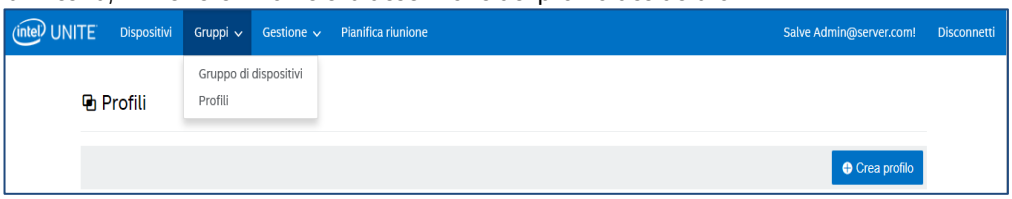


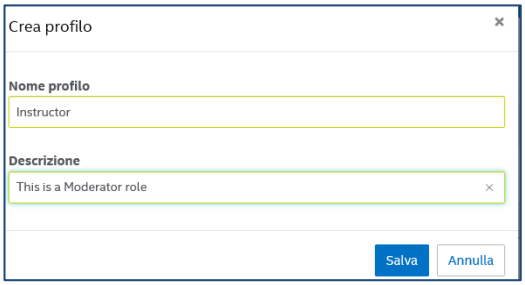
Fare clic su **Aggiungi moderatore** per inserire manualmente il **Nome** e l'**Indirizzo e-mail** del moderatore. Alla fine dell'operazione, fare clic su **Salva**.



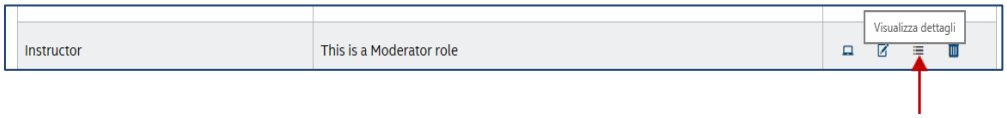
La modalità per la funzionalità Moderatore deve essere impostata sul profilo dell'hub, così da predisporre un ambiente misto sui sistemi. Continuare seguendo la procedura seguente:

- Accedere alla pagina **Gruppi** e selezionare **Profili**, quindi fare clic su **Crea profilo.** Quando si apre la finestra, immettere il nome e la descrizione del profilo desiderato.

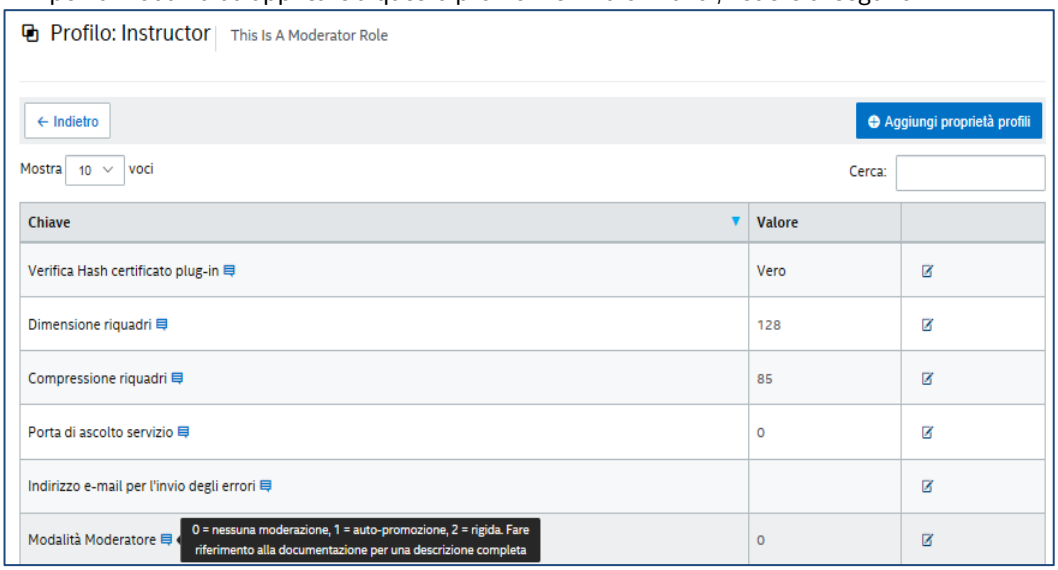




- Una volta creato il profilo, individuarlo nell'elenco e, nella colonna destra accanto al profilo, fare clic su Visualizza dettagli.



- Nella colonna **Chiave**, individuare la chiave **Modalità Moderatore** e immettere il **Valore** desiderato per la modalità da applicare a questo profilo. Per i valori validi, vedere di seguito:



Valori e descrizione moderatore:

0- **Non gestito**: modalità predefinita. Nessun Moderatore nelle riunioni/sessioni. Tutti i partecipanti sono egualmente autorizzati a visualizzare e presentare contenuti. Le versioni precedenti del software Intel Unite (fino alla versione v3.1) utilizzavano questa modalità.

1- **Auto-promozione**: la riunione/sessione non è gestita finché un partecipante non si promuove al ruolo di Moderatore. In questo caso, solo il Moderatore può designare un altro partecipante come Moderatore. Il Moderatore può anche designare il relatore della sessione.

2- **Rigida**: la riunione/sessione è gestita solo dal Moderatore designato. Quando un Moderatore accede alla sessione, viene promosso automaticamente a questo ruolo.

Note:

a. L'elenco dei Moderatori è gestito dall'amministratore IT tramite il portale di amministrazione. L'autenticazione dei Moderatori utilizza una chiave associata all'indirizzo di posta elettronica. Quando un utente viene promosso a Moderatore, il portale di amministrazione gli invia un messaggio e-mail che contiene un URI sul quale fare clic per installare il token Moderatore sul proprio client. Gli utenti devono completare questa procedura una sola volta per ogni sistema.

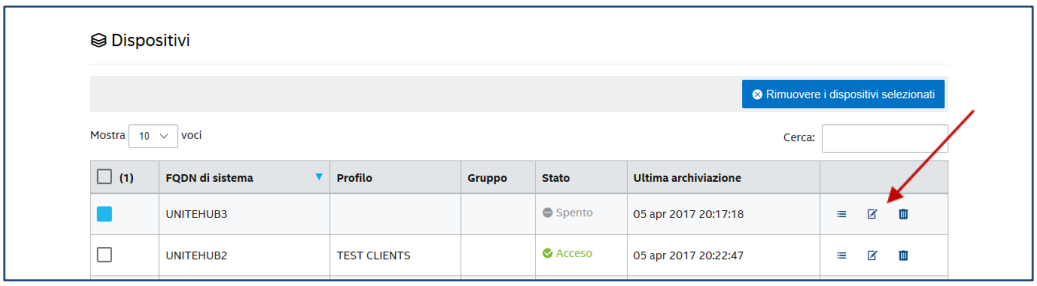
b. L'amministratore IT può revocare i diritti di un Moderatore rimuovendo il token dell'utente dal portale di amministrazione.

c. Se si desidera inviare messaggi e-mail ai Moderatori riguardo alla registrazione, è necessario che il reparto IT configuri un relay SMTP per consentire il funzionamento di questa funzione.

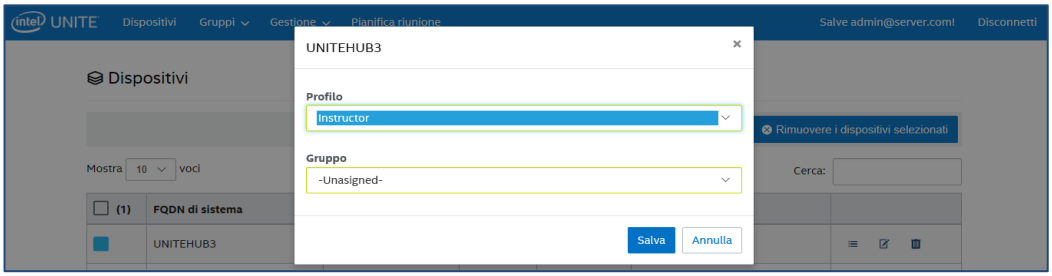
d. Se non si dispone di un relay SMTP ed è quindi necessario generare manualmente l'URI inviato nel messaggio e-mail, procedere come segue:
Accedere alla scheda **Gestione** e selezionare **Proprietà del server**. Fare clic sul collegamento **Modifica,** accanto a **EmailServer,** e quindi specificare il relay SMTP, ad esempio: smtp.example.com:22

È possibile configurare solo i relay SMTP che non richiedono l'autenticazione. Inoltre è possibile ottenere e installare manualmente il token della modalità moderatore per un utente. Per ulteriori dettagli, consultare la sezione **Installazione manuale del token relativo** alla modalità Rigida.

- Per abilitare il profilo di moderatore su un hub selezionato, accedere alla pagina **Dispositivi**, selezionare dall'elenco l'hub che si desidera configurare e fare clic sul collegamento **Modifica** situato nella colonna destra.



- Quando si apre la finestra, selezionare il Profilo creato per il Moderatore nella sezione Profilo e il Gruppo a cui appartiene, se presente, quindi fare clic su **Salva**.



Una volta compilato l'elenco dei Moderatori, è possibile eliminare una voce qualsiasi selezionandola (casella blu) e facendo clic su **Elimina**. Per inviare al Moderatore un URL che consente di partecipare alla riunione/sessione come Moderatore, selezionare il nome desiderato e fare clic su **Invia token**.

8.5.4.1 Installazione manuale del token relativo alla modalità Rigida

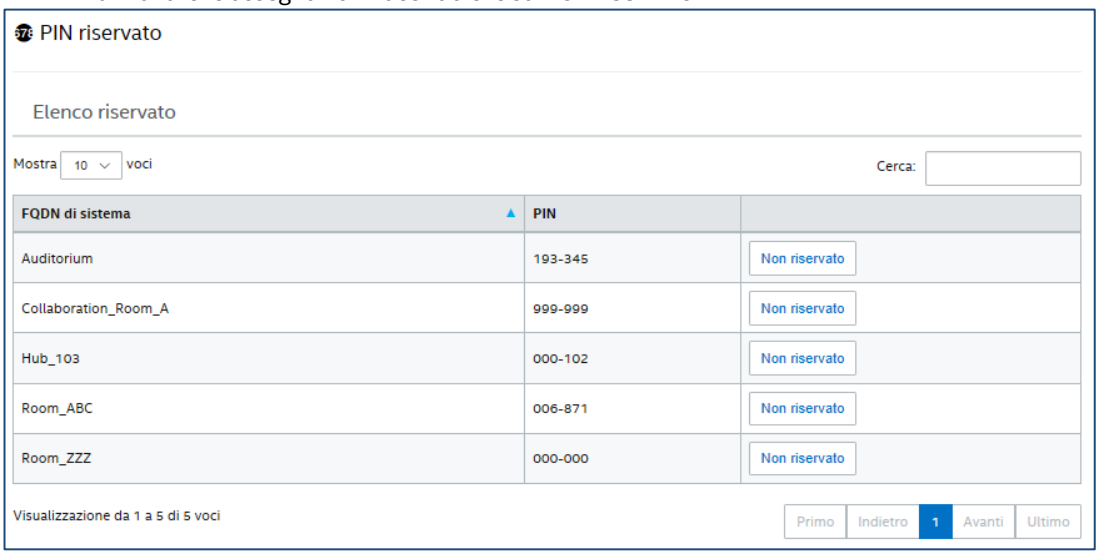
Se non si dispone di un relay SMTP, è possibile ottenere e installare manualmente il token della modalità moderatore per un utente che è stato aggiunto come Moderatore. A tal fine, è necessario installare Microsoft SQL Server Management Studio.
Per ottenere il token:

- Aggiungere un moderatore
- Aprire Microsoft SQL Server Management Studio e connettersi al server di database utilizzando le credenziali di amministratore utilizzate durante l'installazione del server Enterprise
- Espandere "Database", quindi "UniteServer" e infine "Tabelle"
- Fare clic con il pulsante destro del mouse su "dbo.moderatori" e quindi su "Seleziona primi 1000"
- Nei risultati individuare lo "UserName" che corrisponde a quello aggiunto nel passaggio precedente
- Fare clic con il pulsante destro del mouse e copiare il token negli Appunti
- Aprire il blocco note e creare l'URI: intelunite://localhost/SetModerationToken?Token=<incollare il token del passo precedente>
- Accedere a Intel Unite
- Su dispositivi Windows: aprire Esplora risorse, copiare/incollare l'URI completo e premere Invio
- Su dispositivi Mac: aprire Safari, copiare/incollare l'URI completo e premere Invio

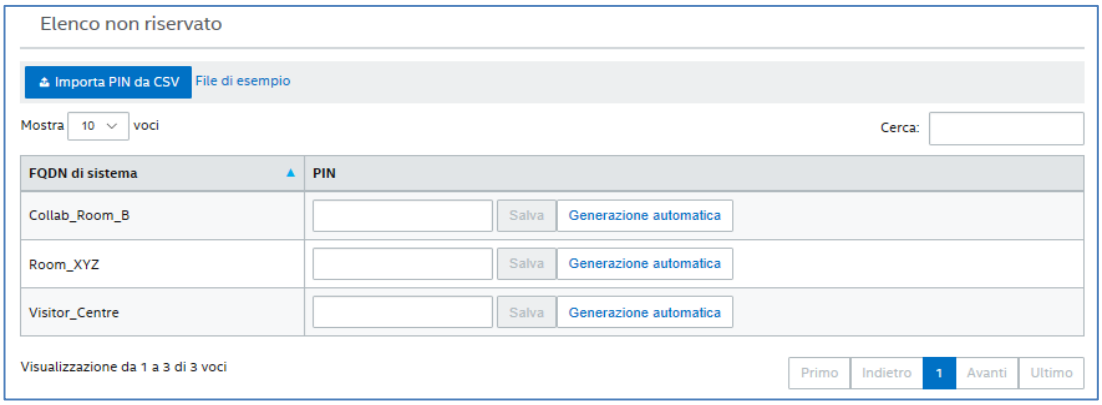
8.5.5 Gestione > PIN riservato

Questa pagina è suddivisa in due sezioni: l'elenco **Riservato** e l'elenco **Non riservato** dei sistemi, che indicano se il PIN visualizzato durante la riunione/sessione è statico o non statico. I sistemi possono essere assegnati dall'amministratore IT in sale prestabilite, dove gli utenti inseriscono lo stesso PIN durante la riunione o la sessione. Questa modalità si distingue da quella predefinita, che prevede un PIN assegnato su rotazione.

- **Elenco Riservato:** questo è l'elenco delle prenotazioni già configurate dal reparto IT. È possibile annullare le assegnazioni facendo clic su **Non riservato**.



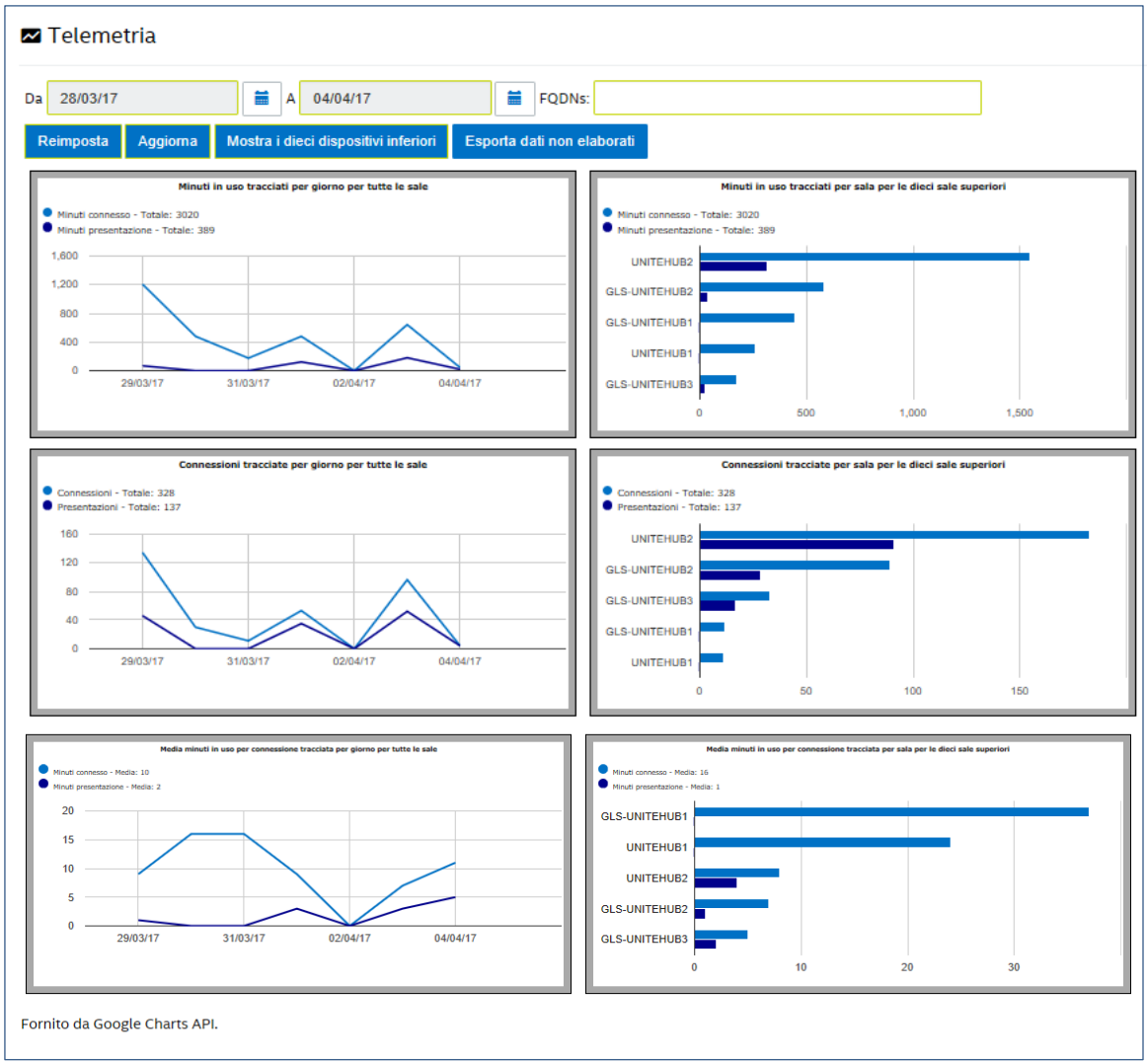
- **Elenco non riservato:** questo è l'elenco dei sistemi che non dispongono di prenotazioni di PIN statici. I PIN possono essere immessi manualmente, generati in modo automatico o importati da un file CSV.



Quando si assegnano i PIN, fare clic su **Salva** per conservare i valori.

8.5.6 Management > Telemetria

Questa pagina mostra i dati di telemetria raccolti tramite il portale di amministrazione. Per visualizzarli, è necessario installare il plug-in di telemetria per la soluzione Intel Unite®. Il plug-in di telemetria consente agli amministratori IT di raccogliere le informazioni sull'utilizzo dell'applicazione Intel Unite e dei dispositivi client collegati a ciascun hub. L'amministratore IT sarà in grado di visualizzare informazioni quali il numero di connessioni in ogni stanza e al giorno, il tempo medio utilizzato per connessione e così via. Per informazioni dettagliate e per distribuire il plug-in nel sistema, fare riferimento alla **Guida al plug-in Intel Unite® di telemetria**.



8.6 Pagina Pianifica riunione

La pagina Pianifica riunione è una funzione che consente di creare un URL di una riunione per i partecipanti di una riunione/sessione che non sono in grado di installare o utilizzare il plug-in Intel Unite esistente per Microsoft Office. Ogni partecipante può visualizzare questa pagina.

Basta fare clic sul pulsante **Genera una nuova riunione** per creare l'URL e inviarlo agli utenti che parteciperanno alla riunione o alla sessione.

8.7 Altre opzioni di configurazione per il portale di amministrazione

8.7.1 Configurazione del profilo

Per configurare i profili, accedere a **Gruppi** > **Profili** e fare clic sui **Dettagli** del profilo nel portale di amministrazione. Le impostazioni di configurazione sono qui visualizzate sotto forma di coppia "Chiave-valore". È possibile modificare tali valori in modo da personalizzare l'applicazione e l'esperienza dell'area della riunione o della sessione. La personalizzazione, ad esempio, può riguardare l'immagine dello sfondo da visualizzare nell'hub, le dimensioni del PIN, il colore carattere e il contenuto.
Dopo la personalizzazione dei valori, assegnare i dispositivi al profilo per applicare le impostazioni di configurazione corrispondenti. Per applicare il profilo ai dispositivi, fare clic sul collegamento **Visualizza dispositivi** e quindi su **Aggiorna elenco dispositivi**. Viene visualizzato l'elenco dei dispositivi. Per applicare le impostazioni di configurazione, fare clic sulla casella di controllo accanto al dispositivo desiderato.

Nella tabella seguente sono riportate le **Chiavi** disponibili, la rispettiva descrizione, il tipo di dati e il valore predefinito delle chiavi.

Chiave	Descrizione	Tipo di dati	Valore predefinito
Consenti trasferimento file	Flag per consentire o impedire a un hub o client di trasferire un file	Booleano	Falso
Supporto streaming audio/video	Flag per consentire agli utenti Windows di presentare l'intero desktop con l'esperienza A/V completa (1080p a 20-30fps)	Booleano	Vero
Modifica il PIN durante la riunione	Bloccare il PIN per una riunione/sessione. In questo modo rimarrà invariato fino a quando tutti gli utenti non saranno disconnessi Vero = consente la modifica del PIN durante la sessione Falso = blocca il PIN durante la sessione	Booleano	Vero

Disattiva visualizzazione remota	Disattivare la funzionalità di visualizzazione remota da alcune sale. Quando l'opzione è impostata, se un utente cerca di accedere ai contenuti utilizzando la visualizzazione remota, si vedrà un'immagine che indica che questa funzionalità non è disponibile Vero = disattiva la visualizzazione remota Falso = attiva la visualizzazione remota	Booleano	Falso
Visualizza dimensioni PIN	Dimensione in pixel. Valore in pixel dell'altezza del PIN sullo schermo (valori più grandi agevolano la lettura del PIN all'altro capo della stanza)	Intero	48
Visualizza trasparenza PIN	Controlla la trasparenza alfa del PIN visualizzato sul monitor 100 = 100% visibile 1-99 = il PIN è visibile all'interno di un riquadro; l'opacità varia a seconda del valore utilizzato 0 = il PIN è trasparente	Intero	100
Estensioni file bloccate, visualizzato come Estensioni file bloccate	Elenco separato da virgola delle estensioni di file bloccate (ad esempio, .exe, .bin, .msi)	Stringa	Vuoto
Dimensione massima file, visualizzato come Dimensione file massima	Dimensione massima dei file da trasferire	Intero	2147483647 byte (intervallo valido: 0-2147483647)
Modalità Sala a schermo intero	Abilita/disabilita la modalità a schermo intero dell'hub Falso: viene visualizzato solo il PIN, in alto a destra Vero: viene visualizzato il PIN, in alto a destra, e uno sfondo schermo intero	Booleano	Falso
Modalità Sala a schermo intero - Colore sfondo	Colore di sfondo utilizzato sull'hub. Colori HTML (colori esadecimali). Esempi di valori validi (valori RGB, formato #000000) sono: Rosso: #FF0000 Giallo: #FFFF00 Verde: #00FF00 Azzurro: #00FFFF Blu scuro: #0000FF Nero: #000000 Bianco: #FFFFFF Grigio: #808080	Stringa	Vuoto (visualizzato in nero)
Modalità Sala a schermo intero - Estensione immagine di sfondo	Flag per impostare l'immagine di sfondo in modo che si estenda sull'intero schermo	Booleano	Falso
Modalità Sala a schermo intero - URL sfondo	Imposta lo sfondo dell'hub sull'immagine (jpg/png) o l'URL specificato. Impostare il valore su Vero per attivare la funzionalità	Stringa	Vuoto

	Esempio: http://serveraziendale.com/background.jpg		
Modalità Sala a schermo intero - Istruzioni	Testo con istruzioni da visualizzare sull'hub. Possibilità di utilizzare {pin} e {host} come sostituzioni URL per il download del client. Il testo specificato viene visualizzato sullo schermo della stanza, nella modalità a schermo intero.	Stringa	{pin}
Modalità Sala a schermo intero - Colore PIN	Colore del PIN visualizzato	Stringa	Vuoto (visualizzato in bianco)
Modalità Sala a schermo intero - Mostra PIN	Visualizza le istruzioni. Impostare il valore su True per attivare la funzionalità	Booleano	Falso
Modalità Sala a schermo intero - Colore testo	Colore del testo visualizzato su hub	Stringa	Vuoto (visualizzato in bianco)
Modalità Sala a schermo intero - Carattere testo	Nome del tipo di carattere per le istruzioni	Stringa	Vuoto
Hub - Blocca tastiera	Blocca le combinazioni di tasti Ctrl-Esc, Alt-Tab, Alt-F4, la barra degli accessi e i tasti Windows nell'hub Se ha valore True, il blocco dell'hub è abilitato. Questa impostazione può essere ignorata specificando la password impostata nella chiave di registro del sistema (valore CHIAVE DI REGISTRO)	Booleano	Falso
Hub - Mostra orologio	Mostra l'orologio nell'angolo inferiore destro	Booleano	Vero
Modalità Moderatore	Per assegnare la modalità Moderatore in una riunione/sessione, utilizzare i seguenti valori: 0 = nessuna moderazione 1 = auto-promozione 2 = rigida	Intero	0
Indirizzo e-mail per l'invio degli errori	Immettere l'indirizzo e-mail al quale l'hub invierà i messaggi di errore	Stringa	Vuoto (visualizzato in bianco)
Porta di ascolto servizio	Una porta assegnata all'hub per l'ascolto delle connessioni in entrata	Intero	0 (0 = porta assegnata automaticamente)
Compressione riquadri	Consente di regolare il rapporto di compressione per la condivisione di contenuti non AV. Percentuale di compressione da applicare a una posizione modificata del display (riquadro) da trasmettere in rete (i valori più elevati utilizzano maggiore larghezza di banda)	Intero	85 (intervallo valido: 5-100)

Dimensione riquadri	Consente di regolare le dimensioni del riquadro per la condivisione di contenuti non AV. Dimensione del riquadro per la suddivisione dello schermo in più parti. Indica la dimensione in pixel di ogni riquadro.	Intero	128 (intervallo valido: 32-512)
Verifica Hash certificato plug-in	I plug-in richiedono una verifica Vero = verifica hash certificato Falso = non verificare hash certificato	Booleano	Vero

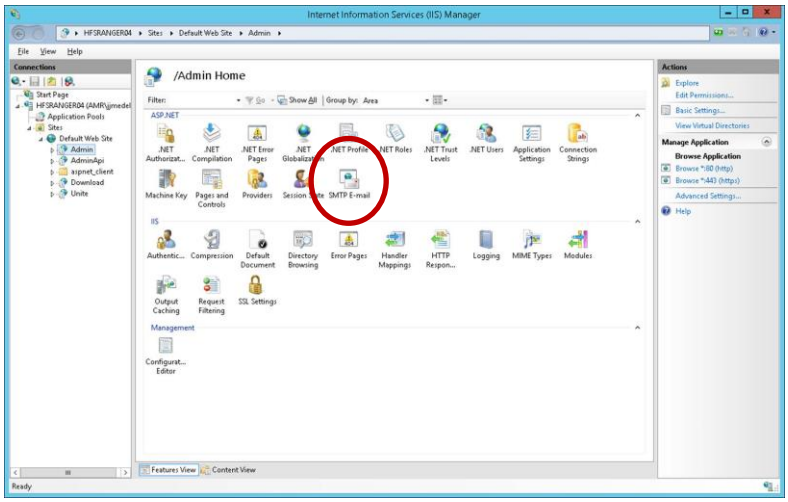
8.7.2 Intervallo di aggiornamento del PIN

L'intervallo predefinito di aggiornamento del PIN è di 5 minuti; questo significa che il PIN visualizzato sull'hub cambia ogni 5 minuti. Può essere impostato su un valore da 2 a 60 minuti, per incrementi di 1 minuto, modificando il file **web.config** nella radice della directory virtuale di servizio Web. È possibile accedervi tramite la gestione IIS, oppure accedendo alla directory Intel Unite\PinServer. Per impostazione predefinita, la posizione di installazione è C:\Program Files (x86)\Intel\Intel Unite\PinServer.
Modificare il valore nel tag <add key="**PinExpireTimeInMinutes**" value="5"></add> impostando l'intervallo di aggiornamento desiderato.

8.7.3 Impostazioni del server di posta elettronica

Il portale di amministrazione definisce il server SMTP nel file xml web.config, creato quando l'applicazione Intel Unite è installata sul server. A seconda della posizione in cui è configurato il server SMTP, è necessario modificare **mailSettings** nel file xml web.config in modo che l'"host" faccia riferimento al server SMTP. Per impostazione predefinita, il file xml Web.config si trova in C:\Program Files (x86)\Intel\Intel Unite\PinServer.
Verificare che il server di posta elettronica SMTP sia configurato in IIS e che l'impostazione sia compatibile con l'applicazione durante la pre-installazione del server Enterprise.
Il file contiene le seguenti impostazioni:

```
<mailSettings>
    <smtp from="noreply@uniteserver.com" deliveryMethod="Network">
        <network enableSsl="false" host="smtp.myco.com" port="25"
        userName="noreply@uniteserver.com" password="pass" />
    </smtp>
</mailSettings>
```



8.7.4 Avvisi e monitoraggio

Il server Enterprise offre servizi di avvisi e monitoraggio. Si tratta di un servizio con accettazione esplicita ed è configurato nel portale di amministrazione.
Tutti i dispositivi configurati per gli avvisi verranno monitorati e, se il check-in non viene effettuato entro la soglia di avvertimento, viene inviato un messaggio e-mail a tutti gli utenti specificati.
Per scegliere di ricevere i messaggi e-mail sui client non attivi, assicurarsi che all'utente nel portale di amministrazione sia stato assegnato il ruolo **Notifications**. Per scegliere di monitorare un dispositivo, aggiungere la chiave **EnableReporting** ai metadati e impostare il valore su **Vero**.
La soglia di avvertimento è configurata in **Gestione** > **Proprietà del server** ed è impostata su 60 minuti come valore predefinito.
InactiveCount (Conteggio client inattivi): se l'utente desidera ricevere un'e-mail immediatamente dopo il controllo successivo, occorre impostare un numero basso.
L'indirizzo e-mail (smtp da) e il server di posta (host) devono essere specificati nel file **clocktower.exe.config**, disponibile in: /productfiles/release/clocktower.exe.config. Per impostazione predefinita, il file xml clocktower.exe si trova in C:\Program Files (x86)\Intel\Intel Unite\ClockTower

Il file contiene le seguenti impostazioni:

```
<mailSettings>
    <smtp from="noreply@uniteserver.com" deliveryMethod="Network">
        <network enableSsl="false" host="smtp.myco.com" port="25"
        userName="noreply@uniteserver.com" password="pass" />
    </smtp>
</mailSettings>
```

9 Controlli di sicurezza per sistema operativo e PC

9.1.1 Standard di sicurezza minimi (MSS, Minimum Security Standard)

È consigliabile che tutti i dispositivi su cui è in esecuzione l'applicazione Intel Unite rispettino gli standard di sicurezza minimi predefiniti dell'organizzazione, abbiano un agente installato per l'applicazione delle patch, nonché un antivirus/IPS/IDS e tutti gli altri controlli necessari in base alla specifica MSS (è stato effettuato un test di compatibilità della suite McAfee per anti-malware, IPS e IDS).

9.1.2 Protezione del computer

È possibile bloccare la UEFI (Unified Extensible Firmware Interface) del computer in modo che esegua l'avvio esclusivamente dal caricatore di avvio di Windows (per impedire l'avvio da dischi USB o DVD). Le impostazioni Execute disable bit e la tecnbologia Intel® Trusted Execution possono essere abilitate e le impostazioni bloccate con una password.

Protezione del sistema operativo Windows: in generale, il sistema deve essere eseguito senza privilegi utenti elevati. È inoltre consigliabile rimuovere il software inutilizzato dal sistema operativo, includendo il software preinstallato e i componenti di Windows non necessari (PowerShell, Servizi di stampa e digitalizzazione, Localizzatore geografico di Windows e i servizi XPS).

Blocco del sottosistema GUI: poiché il sistema non utilizza uno schermo tattile, risulta molto più difficile violare il sottosistema GUI utilizzando solo mouse e tastiera. Per impedire che un utente non autorizzato colleghi un dispositivo HID (tastiera o mouse USB), si consiglia di bloccare le combinazioni di tasti **Alt+Tab**, **Ctrl+Maiusc+Esc** e la barra degli **accessi** a livello di programmazione.

9.1.3 Altri controlli di sicurezza

È consigliabile bloccare in Active Directory l'account utente del sistema per uno specifico account di sistema. Se l'implementazione include un numero elevato di unità, è possibile bloccare gli account utente in base a un piano designato di un edificio specifico.

Proprietà del sistema: per ogni sistema, è consigliabile specificare un proprietario designato, che verrà informato in caso di disattivazione del sistema per un periodo di tempo prolungato.
Oltre ai meccanismi di protezione forniti dalla piattaforma Intel vPro e dal software Intel Unite stesso, si consiglia di fare riferimento alle linee guida Microsoft per il consolidamento del sistema operativo Microsoft* Windows*; per dettagli, consultare il documento Microsoft Security Compliance Manager* (SCM) disponibile al seguente collegamento: https://technet.microsoft.com/en-us/solutionaccelerators/cc835245.aspx
Nota: le informazioni riportate nel collegamento rimandano a uno strumento di protezione basato su una procedura guidata, che comprende le procedure ottimali per il consolidamento e la relativa documentazione.

10 Manutenzione

È responsabilità dell'azienda e dell'amministratore IT stabilire un programma di manutenzione regolare. È consigliabile eseguire le seguenti attività di manutenzione:

10.1 Riavvia notturno

È consigliabile riavviare gli hub quotidianamente (preferibilmente in orario notturno) e, prima del riavvio, eseguire attività di manutenzione quali: cancellazione dei file temporanei dalla cache e avvio delle procedure standard di applicazione delle patch.

10.2 Strategia di applicazione delle patch

Se disponibile, eseguire il meccanismo standard di applicazione delle patch in modalità non interattiva (senza prompt della GUI), preferibilmente prima del riavvio notturno di cui sopra.

10.3 Reporting

Raccogliere gli indicatori di attività del sistema e creare un report su misura, in base alle esigenze della propria organizzazione.

10.4 Monitoraggio

Utilizzare un sistema di monitoraggio dell'integrità basato sull'heartbeat del computer ed effettuare un'analisi del tempo di attività dei backend in base alle esigenze.

10.4.1 Monitoraggio dei backend:

Utilizzare strumenti di monitoraggio standard per i server virtuali, per generare e inviare avvisi al supporto di secondo livello.

11 Soluzione Intel Unite per macOS

11.1 Background

Il software Intel Unite per macOS è un tipo di pacchetto di app primarie, in grado di sfruttare specifiche preferenze di valori IT. L'app può così supportare numerose implementazioni comuni, dalle tecniche generali e dai software gestionali Mac all'installazione manuale e all'impostazione delle preferenze.

11.2 Flusso di lavoro generale delle connessioni

Per impostazione predefinita, l'app ricorre al rilevamento automatico DNS (record di servizio DNS) per individuare il server Enterprise più adatto per la connessione. Il flusso di lavoro complessivo è il seguente:

- (Facoltativo) Server Enterprise definito nelle preferenze
- Rilevamento automatico per i seguenti domini:
  - _uniteservice._tcp
  - _uniteservice._tcp.yourSubDomain.yourDomain.yourTLD
    i. Esempio: _uniteservice._tcp.corp.acme.com
  - _uniteservice._tcp.yourDomain.yourTLD
    i. Esempio: _uniteservice._tcp.acme.com
  - Tentativo di connessione a HTTPS e quindi a HTTP in caso di errore
- uniteservice.yourDomain.yourTLD

11.3 Valori delle preferenze

Il reparto IT può modificare e personalizzare l'app Intel Unite in modo che possa soddisfare esigenze specifiche in materia di infrastrutture o sicurezza. A tale scopo, impostare le seguenti impostazioni di com.intel.Intel-Unite.plist nella cartella ~/Library/Preferences di ogni utente:

- **Definire un server Enterprise predefinito**
  defaults write com.intel.Intel-Unite EnterpriseServer myServer.mydomain.myTLD

- **Definire una chiave pubblica di un server Enterprise per il pinning dei certificati**
  defaults write com.intel.Intel-Unite EnterpriseServerPublicKey "Stringa della chiave pubblica"

- **Forzare un client in modo che accetti solo certificati del server attendibili**
  defaults write com.intel.Intel-Unite ClientOnlyAllowsTrustedCertificates -bool true

- **Forzare un client in modo che esegua la connessione in modalità autonoma**
  defaults write com.intel.Intel-Unite Standalone -bool true

Ogni impostazione può essere configurata o modificata manualmente. Basta aprire il terminale di macOS (/Applications/Utilities) e inserire il comando seguito da un ritorno a capo. Di seguito sono disponibili descrizioni e informazioni dettagliate di ogni comando:

- **Definire un server Enterprise predefinito**
  L'impostazione di un server Enterprise predefinito interrompe l'esecuzione del processo di rilevamento automatico. Se i client Mac risiedono solo sulla rete dell'utente, quest'impostazione può essere utile per aggiungere l'app Intel Unite al server Enterprise specifico, a scopi di sicurezza o risoluzione dei problemi.

- **Definire una chiave pubblica di un server Enterprise per il pinning dei certificati**

Se si desidera aggiungere l'applicazione del client al server Enterprise specifico, a prescindere che si utilizzi il rilevamento automatico, impostare la stringa della chiave pubblica in ogni client. Per acquisire questo valore, procedere come segue:

- Aprire Safari su qualsiasi Mac sulla rete aziendale
- Accedere all'indirizzo HTTPS del server Enterprise
- Fare clic sull'icona di blocco nella barra degli indirizzi
- Fare clic sul pulsante **Mostra certificato** nella scheda del certificato
- Fare clic sul triangolo **Dettagli** per espanderne il contenuto
- Scorrere i dati del certificato fino a trovare il campo **Informazioni sulla chiave pubblica** > **Chiave pubblica**
- Fare clic sul campo di dati che inizia con "256 byte":
- Il campo si espande
- Selezionare tutti i dati nel campo usando il mouse o la combinazione CMD+A
- Copiare i dati negli Appunti selezionando **Copia** dal menu contestuale o **CMD+C**
- Nei comandi predefiniti, sostituire **Stringa della chiave pubblica** con i dati incollati negli Appunti. Nota: i dati devono essere inclusi tra virgolette.

Così come avviene con la definizione di un server Enterprise predefinito, quando si configura questa opzione, la base di utenti incontra difficoltà a connettersi ad altre soluzioni Intel Unite installate presso altri partner o altre posizioni.

- **Forzare un client in modo che accetti solo certificati del server attendibili**
  Oltre a definire un server Enterprise specifico o aggiungere la chiave pubblica del certificato, è possibile impostare l'app Intel Unite in modo da consentire solo le connessioni a server/certificati che sono provvisti di autorizzazione completa, assegnata dalla catena attendibile di certificati. Così facendo, è necessario verificare che il certificato del server Enterprise rimandi a un server root pubblico, come stabilito da Apple nel portachiavi, o che sia stato installato un proprio certificato del server root e qualsiasi altro certificato intermedio necessario su ogni client.

- **Forzare un client in modo che esegua la connessione in modalità autonoma**
  L'impostazione di questa modalità modifica il flusso di lavoro della connessione in modo da rilevare automaticamente l'UDFP di un hub che ha generato un PIN in un ambiente privo di un server Enterprise. In questo scenario il sistema basato su processori Intel Core vPro svolge la funzione di host principale e risulta utile negli ambienti delle piccole e medie imprese, dove può non esserci un reparto IT che possa occuparsi dell'installazione dell'infrastruttura del server Enterprise. Questa modalità funziona solo tra sistemi sulla stessa sottorete in cui non sono bloccati i pacchetti UDP.

11.4 Metodologie comuni di distribuzione

Se si utilizza il rilevamento automatico, la distribuzione può essere eseguita con la massima semplicità trascinando l'applicazione Intel Unite nella cartella Applicazioni. Negli ambienti più complessi o in quelli che richiedono impostazioni di sicurezza aggiuntive, è consigliabile impostare preferenze specifiche in concomitanza con la distribuzione del pacchetto di app. Esistono diversi modi per procedere. Ecco alcuni dei più diffusi:

- Bash script
  - Le impostazioni di preferenza possono essere definite in un Bash script che può essere distribuito agli utenti in concomitanza con il pacchetto di app.
- Pacchetto di installazione personalizzata tramite PackageMaker
  - Le impostazioni di preferenza possono essere definite mediante uno script preliminare o successivo.
- Installazione personalizzata tramite il desktop remoto di Apple
  - Con il desktop remoto di Apple, è possibile installare il pacchetto di app Intel Unite e definire tutte le impostazioni di preferenza tramite il menu **Invia comando UNIX...**.
- Installazione personalizzata tramite un software di gestione Mac di livello enterprise

- È possibile creare un'installazione push o pull personalizzata tramite le più comuni soluzioni di gestione Mac di livello enterprise, tra cui:
    - Casper/Bushel
    - Puppet
    - Munki
    - Chef
    - E così via

12 Risoluzione dei problemi

12.1 Impossibile raggiungere la pagina del portale di amministrazione dopo aver installato l'applicazione Intel Unite sul server

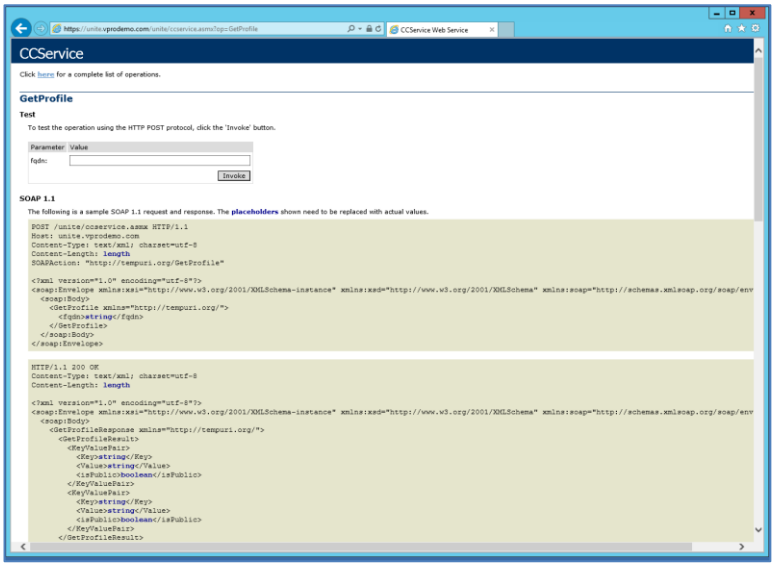
Soluzione: verificare di aver aggiunto al server le funzionalità e i ruoli necessari per il server Web.

- Aggiungere ruoli e funzionalità al server utilizzando Server manager
  - Ruoli server: server Web
    - Includere strumenti di gestione
  - Aggiungere funzionalità di .NET Framework 3.5
  - Aggiungere funzionalità di .NET Framework 4
    - ASP .NET
      - Servizi WCF
      - Attivazione HTTP
    - Ruoli server Web:
      - Server Web, funzionalità HTTP comuni e documento predefinito.

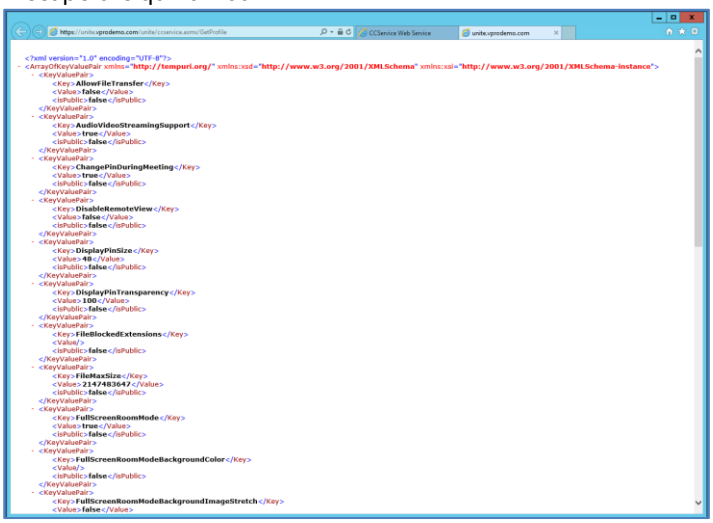
12.2 Impossibile accedere al portale di amministrazione

Quando si tenta di accedere al portale di amministrazione, se si apre una pagina di errore relativa a un problema con un tag xml specifico del file Web.config, rimuovere tale tag dal file Web.config al livello superiore della directory virtuale del portale (accessibile dalla console di gestione IIS).

- Accedere al collegamento seguente per verificare la riuscita dell'installazione del servizio Web:
  https://<nomeserver>/unite/ccservice.asmx
  - Selezionare **GetProfile**.
  - Immettere **test** nel campo **Valore** e premere il pulsante di richiamo.



- Verificare che è possibile visualizzare un profilo predefinito nel file xml, come mostrato in basso. Ciò indica che il servizio PIN può accedere al database e recuperare quindi i dati.



12.3 Errore di avvio dell'applicazione Hub

Una finestra pop up indica l'ID dell'errore. In base all'ID, è possibile determinare la natura dell'errore.

12.3.1 Controllo piattaforma non riuscito con errore ID333333

Questo errore indica che l'hub ha superato un controllo piattaforma, ma non è stato possibile convalidare il certificato di firma codice. Ciò, solitamente, è dovuto a un sistema operativo che non dispone di un certificato radice aggiornato, pertanto il certificato di firma codice Intel Unite pubblico non può essere convalidato.
Assicurarsi che il sistema sia connesso a Internet, aprire un browser e immettere l'indirizzo https://www.microsoft.com (questa operazione forza il sistema ad aggiornare i certificati radice).

12.3.2 Controllo piattaforma non riuscito con errore ID666666

Questo errore indica che la piattaforma non è compatibile con l'applicazione Intel Unite. Controllare con il fornitore OEM se la piattaforma in uso supporta l'esecuzione dell'applicazione.

12.4 L'hub non riceve un PIN dal server PIN. Vengono visualizzati trattini che scorrono

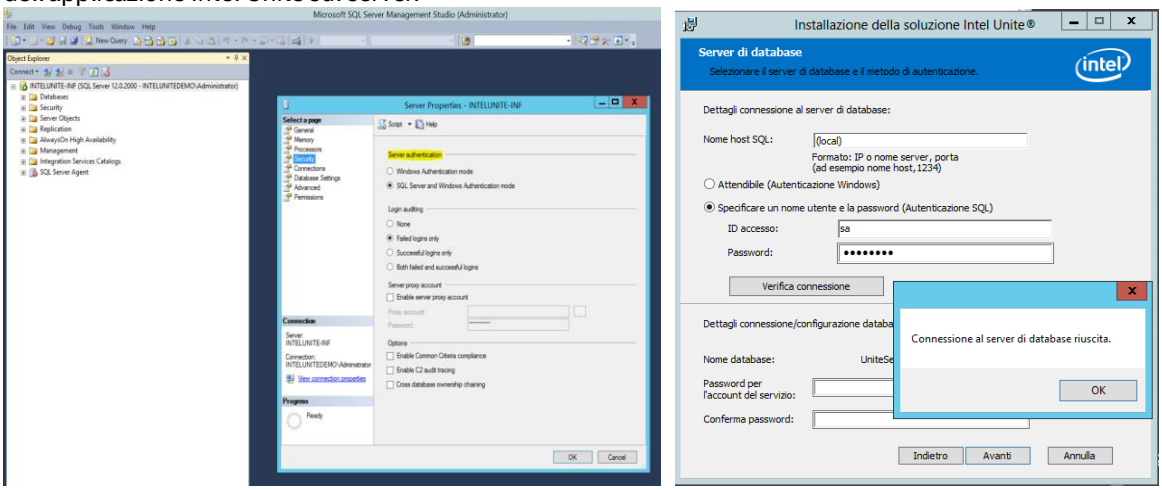
Avviare l'applicazione Intel Unite sull'hub con un parametro debug; ossia, dal prompt dei comandi accedere alla cartella in cui è salvata l'applicazione ed eseguire: **IntelUnite.exe** /debug
Si apre una finestra di debug che contiene le informazioni sulla connessione. Di seguito sono elencati alcuni degli errori e delle soluzioni più comuni. Se le informazioni di debug segnalano uno di questi errori, attenersi alla soluzione specificata per risolvere il problema e ottenere un PIN sull'hub.

12.4.1 Il server non è riuscito a elaborare la richiesta; accesso non riuscito per l'utente "UniteServiceUser"

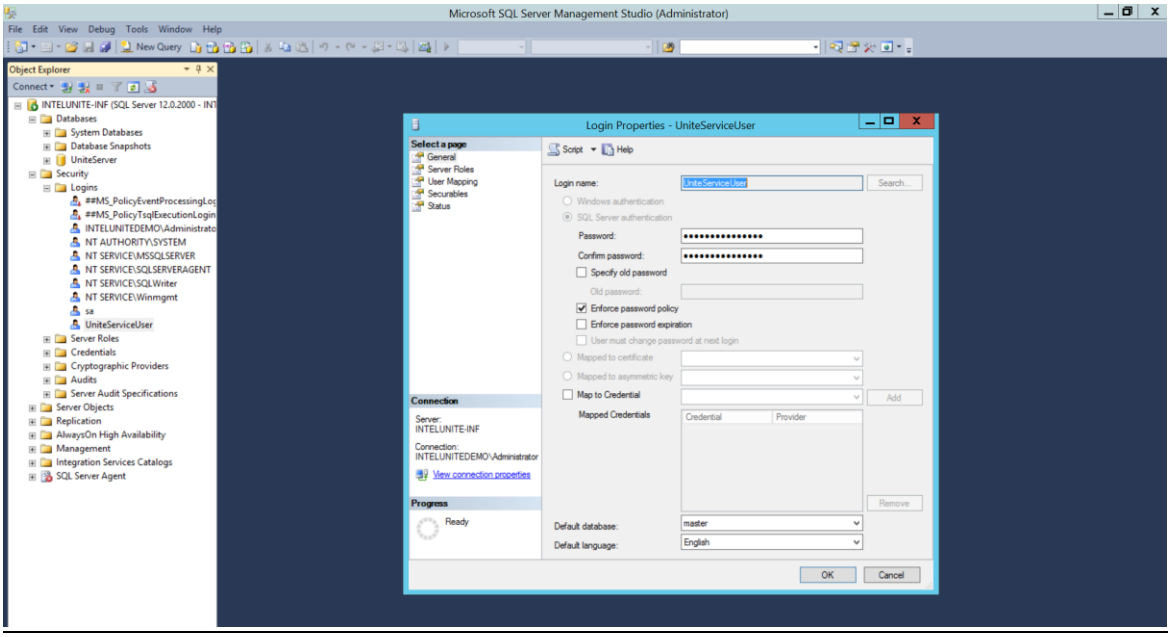
Questo problema può verificarsi se manca corrispondenza nelle credenziali di accesso a SQL o se la password del database viene danneggiata perché un utente tenta di installare più volte il server Enterprise.

Soluzione:

Verificare le modalità di autenticazione utilizzate durante l'installazione di Microsoft SQL. Per modificare il tipo di accesso/autenticazione, accedere a Microsoft SQL Management Studio, connettersi a SQL server, fare clic su di esso con il pulsante destro del mouse e selezionare Proprietà. Scegliere la pagina della sicurezza e accertarsi che sia selezionata la modalità **SQL Server and Windows authentication (Autenticazione di SQL Server e di Windows)** qualora l'autenticazione di SQL sia stata selezionata durante l'installazione dell'applicazione Intel Unite sul server.



Se il problema persiste, reimpostare la password di **UniteServiceUser**. Con Microsoft SQL Management Studio connettersi a SQL server, accedere a **Security (Sicurezza)** > **Logins (Accessi)** e fare clic con il pulsante destro del mouse su **UniteServiceUser** per aprire la finestra **Login Properties (Proprietà account di accesso)**. Inserire una nuova password e fare clic su **OK** per salvare le modifiche.



12.4.2 Nessun server in elenco. Provare il record di servizio DNS: _uniteservice._tcp

Soluzione:

Il problema può verificarsi se l'hub non riesce a trovare il record DNS. In fase di debug, aprire la finestra della riga di comando ed eseguire il comando nslookup. Verificare che l'hub sia in grado di eseguire il ping del server su cui è in esecuzione il servizio DNS e che sia stato creato un record di servizio DNS per la soluzione Intel Unite. Il record di servizio deve presentare i seguenti valori: **Service (Servizio)**: _uniteservice, **Protocol (Protocollo)**: _tcp, **Port number (Numero porta)**: 443 e **Host offering this service: (Host che offre questo servizio:)** FQDN del server Enterprise.

12.4.3 Impossibile stabilire relazioni di trust per il canale sicuro SSL/TLS con l'autorità "uniteserverfqdn"

L'ultima versione della soluzione Intel Unite accetta solo certificati SHA-2 o versione successiva. Controllare con il reparto IT per verificare che il certificato del server Web attendibile emesso sia un certificato SHA-2 e che il percorso di certificazione sia valido.
Per un ambiente di test, ottenere un certificato SHA-2 o disattivare la crittografia nell'ambiente.

- Per utilizzare Unite senza crittografia, ignorare i passaggi successivi che forniscono dettagli su Site Bindings (Binding sito) per la porta sicura 443 e procedere con l'installazione del server MS SQL e la preparazione del record del servizio DNS. È necessario, inoltre, accertarsi che il servizio sia disponibile sulla porta 80 quando si crea un record del servizio DNS.
- Un altro modo per ignorare il controllo del certificato consiste nell'aggiungere il registro nell'account di sistema dell'hub e del client.
  HKEY_LOCAL_MACHINE\software\Intel\Unite\AllowInsecureCertificates (DWORD) [1 se il controllo dell'algoritmo del certificato deve essere ignorato, 0 negli altri casi. (se il valore è 0, viene forzato l'uso di un certificato SHA2 da parte del certificato Enterprise)]

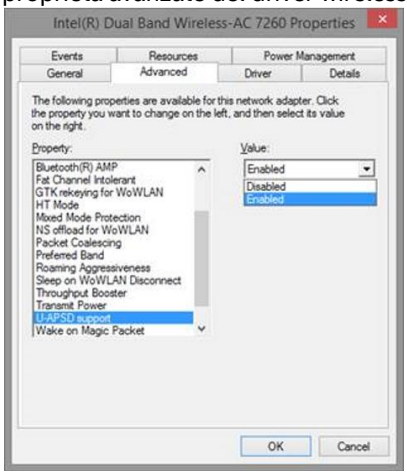
12.5 Arresto anomalo dell'applicazione client all'avvio e/o alla connessione

Eseguire l'applicazione client con un parametro debug e salvare le informazioni in un file di registro (eseguire Intel Unite.exe /debug >logfile.txt).
Se il file di registro contiene il messaggio "ECCEZIONE: - Chiave non utilizzabile nello stato specificato.", chiudere l'applicazione ed eliminare il file C:\Users\eaviles\AppData\Roaming\Microsoft\Crypto\RSA\[sid]\d046df

12.6 Attenzione: l'utente potrebbe notare tempi di connessione più lunghi del solito o un rallentamento degli aggiornamenti dello schermo.

Causa principale:

Si tratta di un bug relativo ad alcuni punti di accesso wireless quando è attivato U-APSD (Unscheduled Automatic Power Save Delivery). Consultare www.intel.it/content/www/it/it/support/network-and-i-o/wireless-networking/000005615.html.
Soluzione: questo problema potrebbe essere risolto con un aggiornamento del firmware dei punti di accesso wireless. Nella maggior parte delle imprese, questa operazione risulta difficile; come ultima risorsa, disattivare U-APSD sul client, nelle proprietà avanzate del driver wireless.



12.7 Attenzione: rallentamento del server PIN

Soluzione: il server Enterprise gestisce l'allocazione dei pin e li ricerca per connetterli alle sale. Per motivi di sicurezza, la frequenza con cui un utente può richiedere pin e pin di query dal database è limitata con un algoritmo di backoff esponenziale. Il meccanismo di backoff tiene traccia dei tentativi in base al numero degli stessi e all'indirizzo IP dell'utente.

I server di produzione potrebbero utilizzare servizi di bilanciamento del carico per agevolare la gestione dei carichi e assicurare ridondanza nell'ambiente. I servizi di bilanciamento del carico reindirizzano il traffico ai server Web appropriati. In questo modo sembra che il server Web riceva tutte le richieste dallo stesso indirizzo IP, situazione che attiva quindi gli algoritmi di backoff.

Nel database è presente una stored procedure (*spGetPinBackoffTime*) che restituisce il ritardo calcolato (in secondi) al server Web. Con questa funzionalità disattivata, la stored procedure restituisce sempre 0 e l'algoritmo di backoff viene disabilitato.

12.8 Risoluzione dei problemi di un client Mac

Avviare l'applicazione Intel Unite (/Applications/Utilities) dal terminale per visualizzare i messaggi di debug.
/pathToUnite/Intel\ Unite.app/Contents/MacOS/Intel\ Unite
L'applicazione viene avviata e le informazioni di debug vengono visualizzate nel terminale.

12.8.1 Errore di connessione al server Enterprise -1003: impossibile trovare un server con il nome host specificato.

Soluzione: verificare di aver definito correttamente il dominio di ricerca DNS.
Se un utente definisce un server DNS ma non specifica alcun dominio di ricerca, quando il MAC tenta di eseguire il rilevamento automatico, non è disponibile alcun suffisso di dominio DNS in cui eseguire la ricerca. Se non è stato definito alcun dominio di ricerca DNS, l'applicazione Intel Unite non può aggiungerlo al rilevamento automatico o alla voce "statica" di *uniteservice*. Pertanto, a meno che il rilevamento automatico non funzioni in *_uniteservice._tcp*, il client non sarà in grado di individuare il server Enterprise.
La soluzione più semplice consiste nell'aggiungere un dominio di ricerca DNS (che deve corrispondere al record SRV DNS); in alternativa, è possibile definire il server Enterprise nelle impostazioni *plist*.
Utilizzare il comando del terminale:
defaults write com.intel.Intel-Unite EnterpriseServer myServer.mydomain.myTLD

12.8.2 Errore di connessione al server Enterprise -1001: timeout della richiesta

Soluzione: l'errore può essere dovuto a due cause.

1. Potrebbe esserci un problema con il servizio Web sul server Enterprise.
2. Si è verificato un problema di rete durante la connessione del Mac al server.

Il primo passaggio per la risoluzione del problema consiste nell'individuare il servizio Web nel registro di debug. Cercare https://yourserver/Unite/CCService.asmx.
Copiare e incollare l'URL in Safari e confermare che il Mac è in grado di raggiungere il servizio Web. Questa procedura consente di verificare la presenza di un problema di rete durante la connessione al server e di controllare che il servizio Web sul server Enterprise sia in esecuzione.

12.8.3 Errore di connessione server Enterprise -1200: si è verificato un errore SSL e non è possibile stabilire una connessione sicura con il server.

Consultare il reparto IT per ottenere i certificati SHA-2 validi necessari per la soluzione Intel Unite.

12.9 L'app Intel Unite per i sistemi operativi Mac viene rimossa/disinstallata dal dispositivo client per consentire l'installazione di una versione alternativa o più aggiornata. Tuttavia, vengono conservate le proprietà dell'installazione precedente.

L'applicazione Intel Unite per dispositivi client Mac seguono le convenzioni generali per i sistemi OS X, pertanto le impostazioni utente non vengono rimosse quando l'applicazione viene eliminata.

Soluzione:
Disinstallare l'applicazione Intel Unite dal dispositivo client. Sono disponibili due modi per rimuovere tali impostazioni e ripristinare lo stato originario.

1. Nel terminale (/Applications/Utilities), immettere il seguente comando:

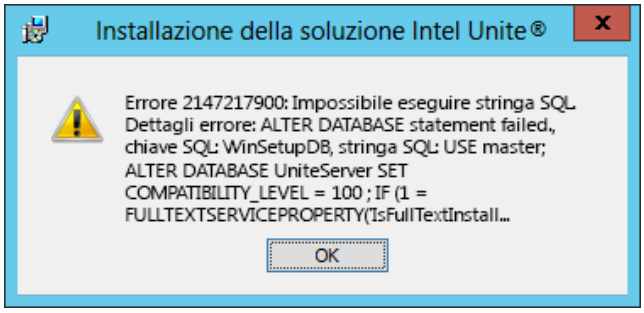
   defaults delete com.intel.Intel-Unite

2. Dal Finder, eliminare il file ~/Library/Preferences/com.intel.Intel-Unite.plist, quindi

   riavviare il sistema. Attualmente, il sistema operativo memorizza i file Plist nella cache, quindi di solito non è possibile eliminarli e consentire al sistema operativo di selezionare la modifica.

12.10 Errore 2147217900: impossibile eseguire stringa SQL.

Questo errore viene generato quando si esegue il programma di installazione del server Intel Unite e il database Unite esiste già, ma il nome del server è vuoto.



Soluzione:
Il programma di installazione genera un errore se il database esiste già nel cluster. Per risolvere questo errore, eliminare il database, assicurarsi di disporre dei diritti di DBAdmin ed eseguire nuovamente il programma di installazione.

12.11 Messaggio di errore: "Errore del database"

Se un amministratore IT sceglie l'opzione "Invia Token" dalla console di amministrazione e riceve il messaggio di errore "Errore del database", è probabile che le impostazioni del server SMTP siano errate. È quindi necessario verificare le impostazioni del server di posta elettronica SMTP.

12.12 Il portale Web di amministrazione non viene visualizzato correttamente (componenti mancanti)

Dopo l'esecuzione di un aggiornamento del software Intel Unite, il portale Web di amministrazione non viene visualizzato completamente poiché mancano alcuni componenti quali caselle di testo, opzioni o icone. Ciò è dovuto al blocco dei tipi MIME causato dall'opzione di filtro richieste in IIS.

Soluzione:

1. Aprire Gestione IIS.
2. Visualizzare le proprietà per il server IIS.
3. Fare clic su **Tipi MIME**, quindi aggiungere l'estensione JSON:
   - Estensioni del nome del file: .json

- Tipo MIME: application/json

4. Tornare alle proprietà del server IIS.
5. Fare clic su **Mapping gestori**.
    - Aggiungere un mapping di script
    - Percorso della richiesta: *.json
    - Eseguibile: C:\WINDOWS\system32\inetsrv\asp.dll
    - Nome: JSON
6. Nel pannello **Connessioni**, andare alla connessione, sito, applicazione o directory per cui si desidera modificare le impostazioni del filtro richieste.
7. Nel pannello **Pagina iniziale**, fare doppio clic su **Filtro richieste**.
8. Individuare Consenti estensione di file
9. Aggiungere le 4 estensioni seguenti:
    - .json
    - .less
    - .woff
    - .woff2

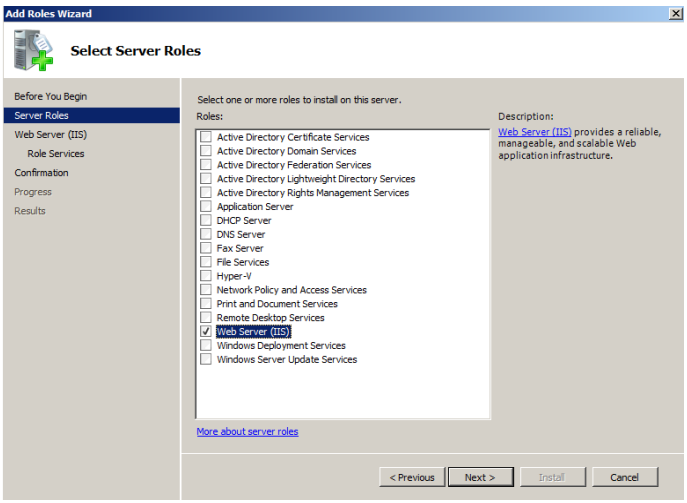
Appendice A. Preparazione per il server Enterprise

Attivazione IIS

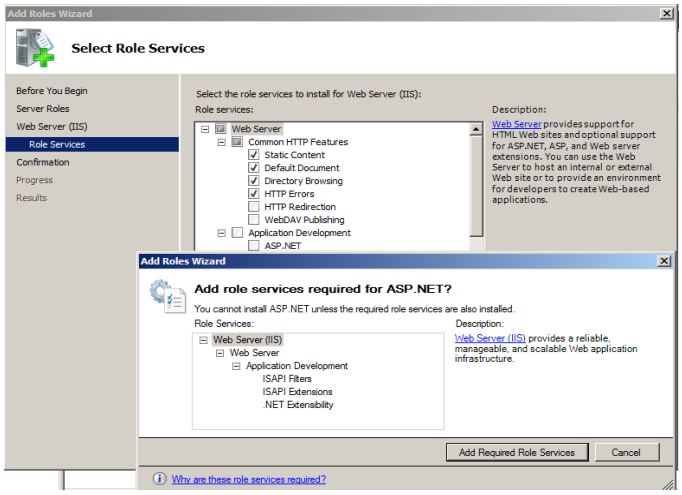
Per Windows 2008:

In Windows Server 2008, è necessario scaricare l'aggiornamento di .NET Framework 4.5 (https://www.microsoft.com/en-us/download/details.aspx?id=40779)

- Fare clic su **Start**, posizionare il cursore su **Administrative Tools (Strumenti di amministrazione)**, quindi fare clic su **Server Manager**.
- In **Roles Summary (Riepilogo ruoli)**, fare clic su **Add Roles (Aggiungi ruoli)**.
- Utilizzare la procedura **Add Roles Wizard (Aggiunta guidata ruoli)** per aggiungere il ruolo **Web Server (Server Web) (IIS)** (contrassegnare la casella).



- Fare clic su **Next (Avanti)** finché non si aprirà la finestra **Select Role Services (Selezione servizi ruolo)**.
- Nella sezione **Application Development (Sviluppo di applicazioni)**, verificare che ASP.NET sia contrassegnato. In caso contrario, selezionarlo. Tenere presente che per impostazione predefinita ASP.NET non è selezionato. **Aggiungi servizi ruolo necessari** per ASP.NET. È richiesto ASP.NET 4.5.



- Una volta creato il ruolo, nel menu **Roles (Ruoli)**, andare a **Web Server (Server Web) (IIS)**, a destra nel riquadro, quindi accedere a **Internet Information Services (IIS) Manager (Gestione Internet Information Services) (IIS)** e selezionare il server in uso nel riquadro a sinistra **Connections (Connessioni)**.

  Riferimento: collegamento alla libreria del server Windows Installazione di IIS su Windows Server 2008

  Nota: l'ultima versione della soluzione Intel Unite accetta solo certificati SHA-2 o versione successiva. Controllare con il reparto IT per verificare che il certificato del server Web attendibile emesso sia un certificato SHA-2 e che il percorso di certificazione sia valido.

  Per un ambiente di test, consultare il team dell'Autorità di certificazione per ottenere un certificato SHA-2 o disattivare la crittografia.
  - Per utilizzare Unite senza crittografia, ignorare i passaggi successivi che forniscono dettagli su Site Bindings (Binding sito) per la porta sicura 443 e procedere con l'installazione del server MS SQL e la preparazione del record del servizio DNS. È necessario, inoltre, accertarsi che il servizio sia disponibile sulla porta 80 quando si crea un record del servizio DNS.
  - In alternativa, è possibile ignorare il controllo del certificato aggiungendo la chiave di registro nell'account di sistema dell'hub e del client. HKEY_LOCAL_MACHINE\software\Intel\Unite\AllowInsecureCertificates (DWORD) [1 se il controllo dell'algoritmo del certificato deve essere ignorato, 0 negli altri casi. (se il valore è 0, viene forzato l'uso di un certificato SHA2 da parte del certificato Enterprise)]

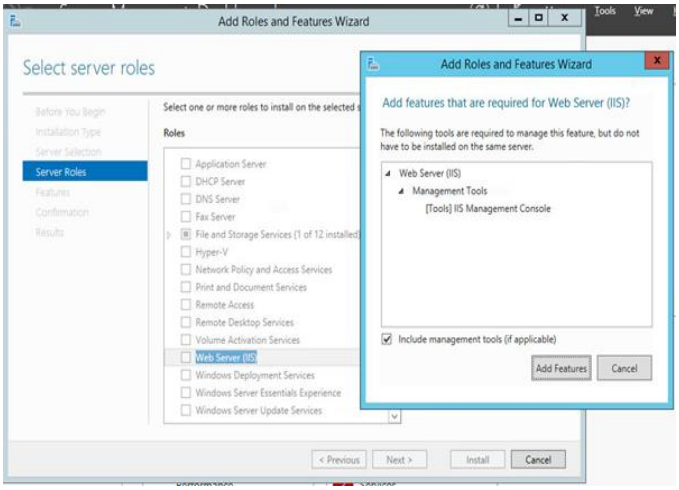
- Per assegnare il certificato, nel riquadro a sinistra **Connessioni**, espandere Siti e fare clic su **Sito Web predefinito**.
- Nel riquadro a destra **Actions (Azioni)**, selezionare **Bindings (Binding)**, sotto Edit Site (Modifica sito).
- Nella finestra **Site Bindings (Binding sito)**, fare clic su **Add (Aggiungi)**.
- Utilizzare le seguenti informazioni:
  - Tipo: https (NB: non "http")
  - Indirizzo IP: tutti non assegnati
  - Porta: 443
  - Nome host: (lasciare vuoto)
  - Certificato SSL: utilizzare il certificato SSL installato nei passaggi precedenti.

Fare clic su **OK**.

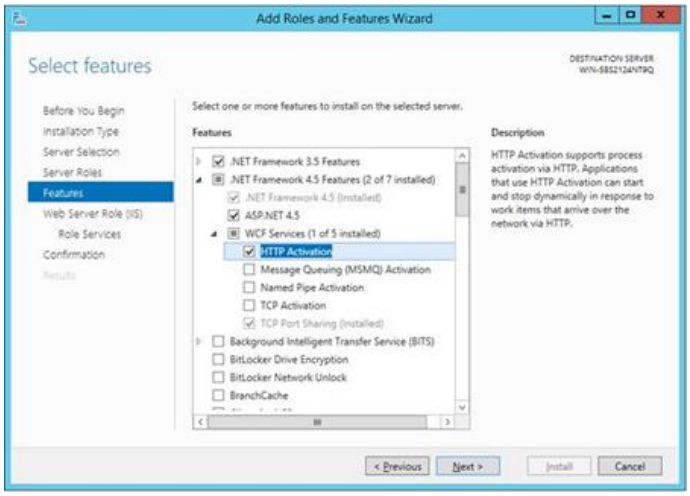
Windows 2012:

- Aprire **Server Manager**.
- Nel menu **Manage (Gestione)**, selezionare **Add Roles and Features (Aggiungi ruoli e funzionalità)**.
- Selezionare **Role-based or Feature-based Installation (Installazione basata sui ruoli o basata sulle funzionalità)**.
- Selezionare il server corretto (per impostazione predefinita, è selezionato "locale").
- Selezionare **Web Server (Server Web) (IIS)**, quindi l'opzione **Add Features (Aggiungi funzionalità)** per le funzionalità richieste dal server Web (IIS), quindi fare clic su **Next (Avanti)**.

NOTA: per ulteriori dettagli relativi alla richiesta di un certificato del server Internet nel server Intel Unite, accedere al seguente collegamento Web di Microsoft https://technet.microsoft.com/en-us/library/cc732906.aspx e ottenere un certificato firmato seguendo la procedura indicata per il fornitore del certificato SSL.

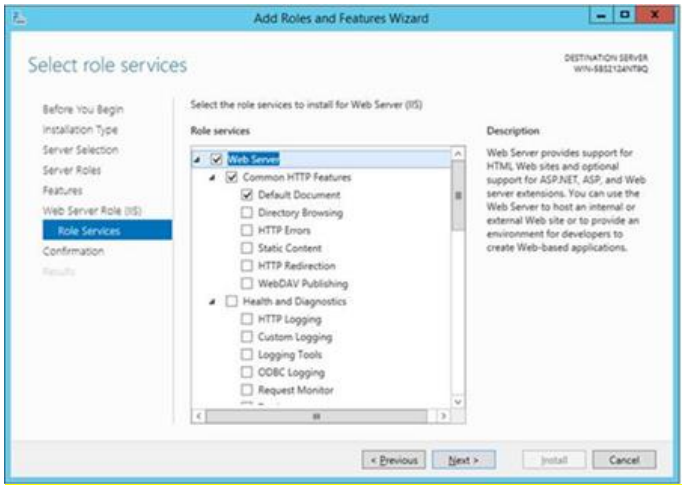


- Nella sezione corrispondente, aggiungere le seguenti funzionalità per IIS (poiché non sono opzioni predefinite):
  - Funzionalità .NET Framework 3.5
  - ASP.NET 4.5
  - Servizi WCF
  - Attivazione HTTP (quando richiesto, aggiungere le funzionalità necessarie per l'attivazione di HTTP) e fare clic su **Next (Avanti)**.



Nota: potrebbe verificarsi un errore di .NET 3.5 durante l'installazione. Indicare un percorso di origine alternativo se il computer di destinazione non può accedere a Windows Update. Fare clic sul collegamento **Specify an alternate source path (Specificare un percorso di origine alternativo)** per indicare il percorso della cartella **\sources\sxs** sul supporto di installazione. Riferimento: https://technet.microsoft.com/en-us/library/dn482071.aspx

- Nella pagina Servizi ruolo, aggiungere **Ruolo server Web (IIS)** come ruolo per il server o accettare il valore predefinito.
- Selezionare i seguenti servizi ruolo da installare per il server Web:
    - Funzionalità HTTP comuni
    - Documento predefinito



- Fare clic su **Next (Avanti)** per continuare e quindi su **Install (Installa)** nella finestra seguente per installare i ruoli e le funzionalità selezionati.
- Una volta creato il ruolo, nel menu **Ruoli**, andare a **Ruolo server Web (IIS)**, a destra nel riquadro, quindi accedere a **Gestione Internet Information Services (IIS)** e selezionare il server in uso nel riquadro **Connessioni** a sinistra.

Nota: l'ultima versione della soluzione Intel Unite accetta solo certificati SHA-2 o versione successiva. Controllare con il reparto IT per verificare che il certificato del server Web attendibile emesso sia un certificato SHA-2 e che il percorso di certificazione sia valido.

Per un ambiente di test, disattivare la crittografia o creare un certificato SHA 2 autofirmato.

- Per utilizzare Unite senza crittografia, ignorare i passaggi successivi che forniscono dettagli su Site Bindings (Binding sito) per la porta sicura 443 e procedere con l'installazione del server MS SQL e la preparazione del record del servizio DNS. È necessario, inoltre, accertarsi che il servizio sia disponibile sulla porta 80 quando si crea un record del servizio DNS.
- Eseguire il comando PowerShell riportato di seguito come amministratore.
  - New-SelfSignedCertificate –dnsname "nomeserver" –CertStoreLocation cert:\LocalMachine\My ; dove "nomeserver" è il nome di dominio completo (FQDN) del server Enterprise.
- In alternativa, è possibile ignorare il controllo del certificato aggiungendo la chiave di registro nell'account di sistema dell'hub e del client. HKEY_LOCAL_MACHINE\software\Intel\Unite\AllowInsecureCertificates (DWORD) [1 se il controllo dell'algoritmo del certificato deve essere ignorato, 0 negli altri casi. (se il valore è 0, viene forzato l'uso di un certificato SHA2 da parte del certificato Enterprise)]

- Per assegnare il certificato, nel riquadro a sinistra **Connessioni**, espandere Siti e fare clic su **Sito Web predefinito**.
- Nel riquadro a destra **Actions (Azioni)**, selezionare **Bindings (Binding)**, sotto Edit Site (Modifica sito).
- Nella finestra **Site Bindings (Binding sito)**, fare clic su **Add (Aggiungi)**.
- Utilizzare le seguenti informazioni:
  - Tipo: https (NB: non "http")
  - Indirizzo IP: tutti non assegnati
  - Porta: 443
  - Nome host: (lasciare vuoto)
  - Certificato SSL: (selezionare il certificato installato nei passaggi precedenti)
  - Fare clic su **OK**.
- Selezionare **Close (Chiudi)**.

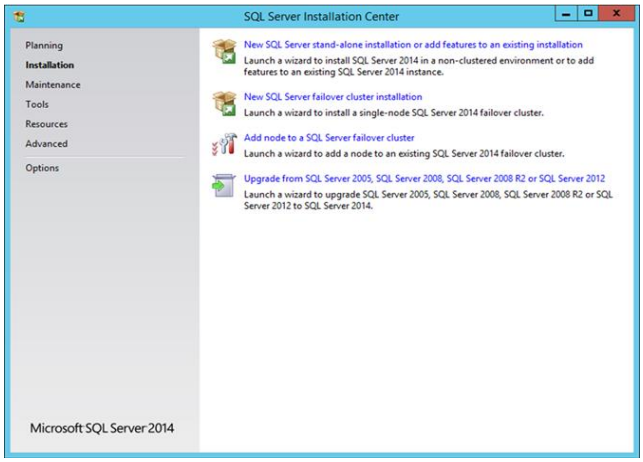
Riferimento: collegamento alla libreria del server Windows Installazione di IIS su Windows Server 2012
Nota relativa alla porta 443: il servizio Web dell'applicazione Intel Unite comunica con i client e gli hub tramite la porta 443; assicurarsi che la porta sia stata attivata come descritto sopra.

Installazione di Microsoft SQL Server

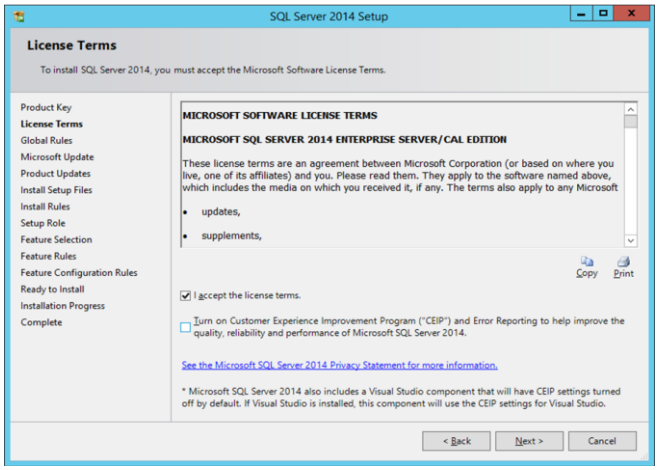
Il server Enterprise richiede l'esecuzione di MS SQL, almeno versione 2008 R2 o successiva. È possibile installare un nuovo SQL server dedicato se si desidera eseguire un “ambiente di test” e utilizzare comodamente l'applicazione; questo passaggio non è tuttavia richiesto. L'applicazione Intel Unite crea un proprio database, tabelle dati e indici all'interno del database esistente, senza interferire con altre tabelle o con i dati esistenti.

Vedere qui di seguito per informazioni sull'installazione di Microsoft SQL 2014

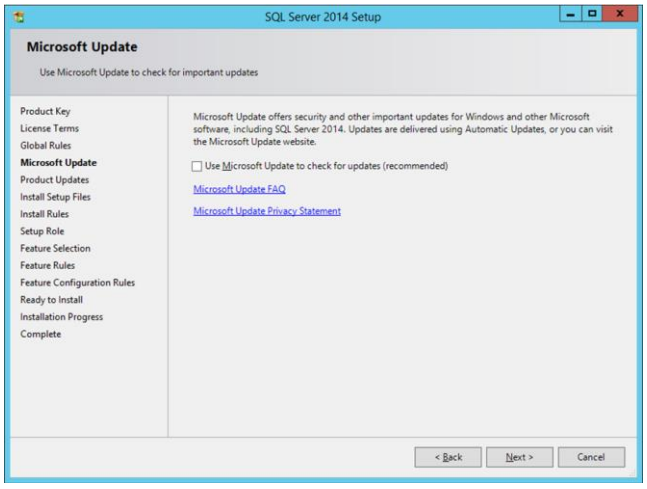
- Avviare l'installazione di SQL server e aprire il relativo centro di installazione. Fare clic su **Installazione** nel riquadro sinistro e selezionare **Nuova installazione autonoma di SQL Server o aggiunta di funzionalità a un'installazione esistente**.



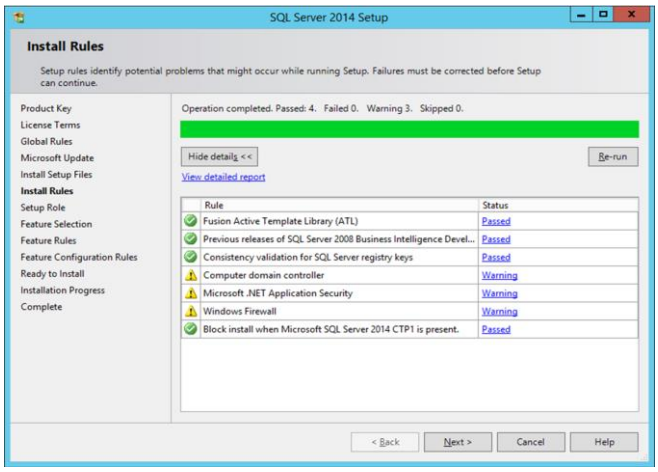
- Immettere la chiave del prodotto, accettare i termini della licenza e fare clic su **Next (Avanti)**.



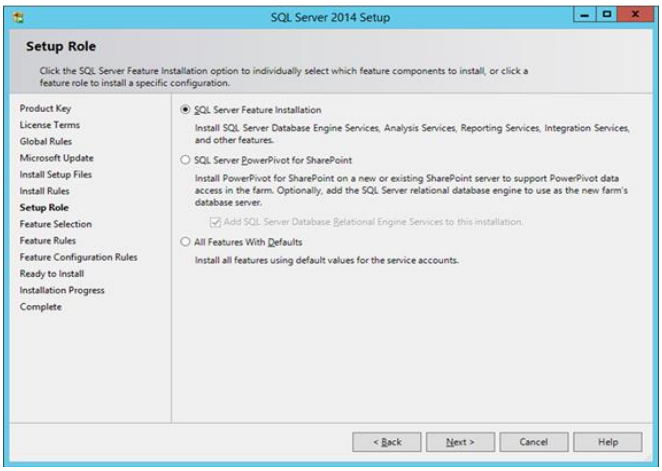
- Selezionare **Use Microsoft Update to check for updates (Utilizza Microsoft Update per verificare la disponibilità di aggiornamenti) (consigliato)** per controllare se sono disponibili aggiornamenti e quindi fare clic su **Next (Avanti)**. Nella finestra successiva la procedura di installazione cerca aggiornamenti del prodotto e installa quelli necessari. Fare clic su **Next (Avanti)** per continuare.



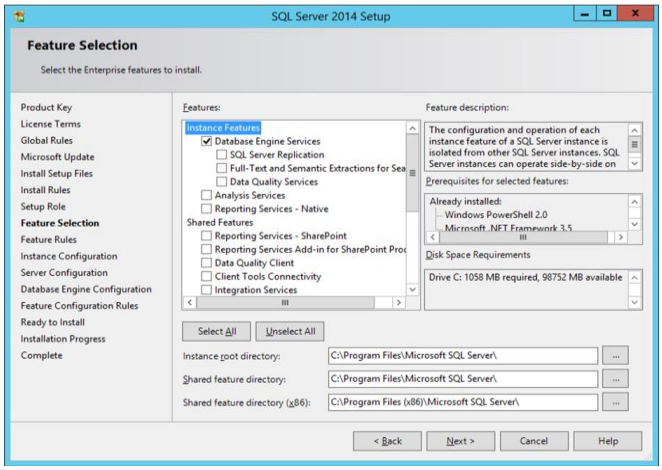
- La procedura di installazione di SQL cerca potenziali errori e requisiti che devono essere soddisfatti prima dell'installazione. Fare clic su **Avanti** per continuare.



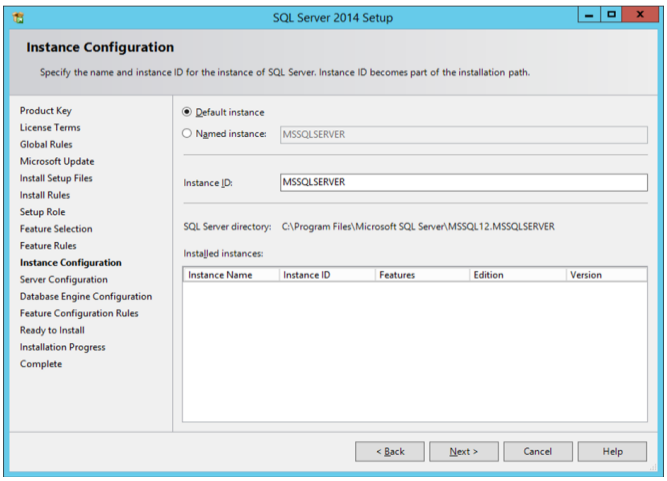
- Selezionare **SQL Server Feature Installation (Installazione funzionalità SQL Server)** e fare clic su **Next (Avanti)**.



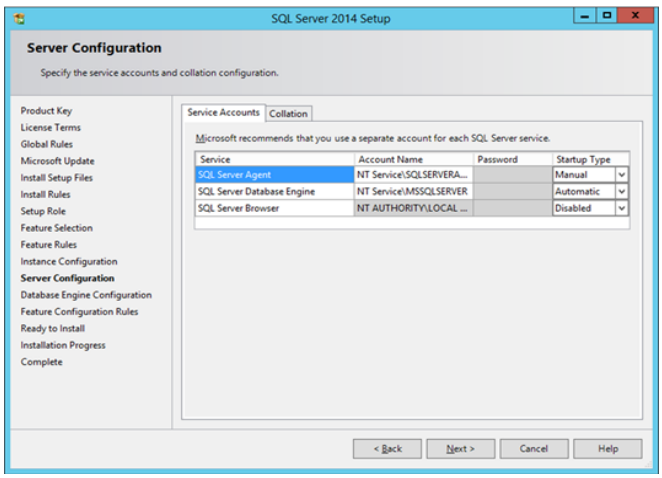
- Nella sezione **Selezione funzioni**, selezionare **Servizi motore di database**, **Strumenti di gestione - Completa** e fare clic su **Avanti**.



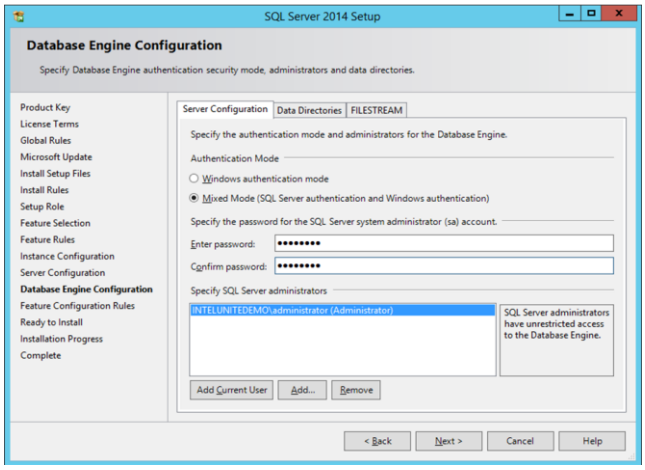
- Specificare il nome e l'ID istanza di SQL server e fare clic su **Next (Avanti)**.



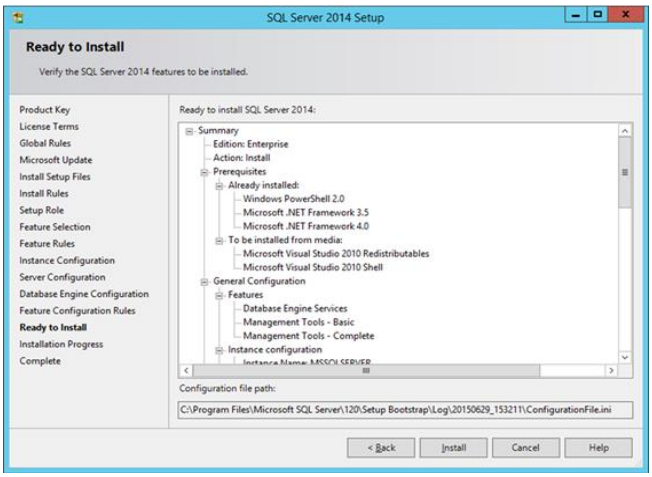
- Specificare gli account di ogni servizio e fare clic su **Next (Avanti)** per continuare.



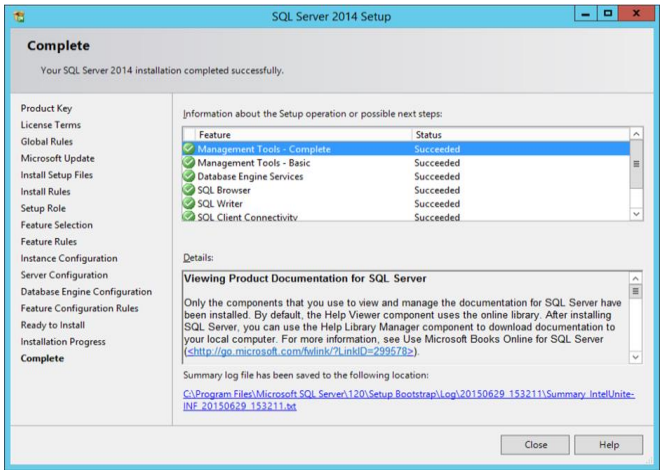
- Selezionare la modalità di autenticazione mista (che comprende l'autenticazione di Windows e di SQL server), specificare gli amministratori di SQL Server e fare clic su **Next (Avanti)**.



- Verificare le funzionalità da installare e fare clic su **Install (Installa)**.



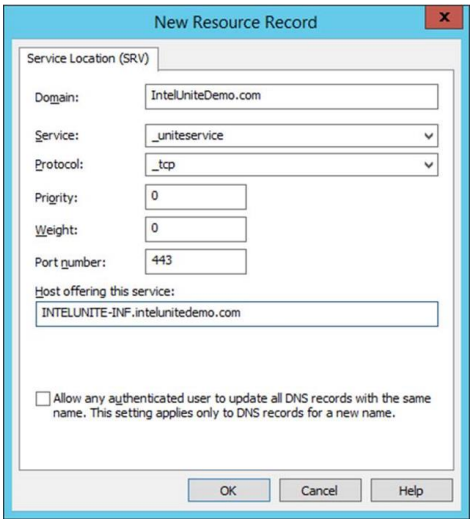
- Fare clic su **Chiudi** per chiudere la finestra di dialogo alla fine dell'installazione.



Creazione di un record di servizio DNS

Durante la ricerca automatica del server Enterprise, l'hub o i client lo individuano utilizzando il servizio DNS. Anche se è possibile utilizzare la ricerca manuale, si consiglia di ricorrere al servizio DNS. Se si prevede di inserire a mano il nome host del server Enterprise durante l'installazione dell'hub e del client, è possibile ignorare questa sezione.
Quando si utilizza un record di servizio DNS, l'hub o il client cerca il servizio denominato _uniteservice._tcp nei record di servizio DNS _uniteservice._tcp.example.com 86400 IN 0 5 443 uniteserver.example.com.
Per aggiungere un record del servizio DNS in Microsoft Windows:

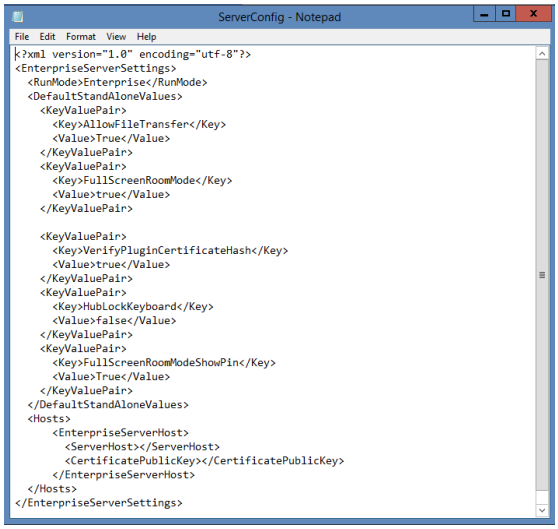
- Sul server DNS, aprire DNS Manager (Gestore DNS).
- Espandere le zone di ricerca diretta (riquadro sinistro).
- Fare clic con il pulsante destro del mouse sulla zona e selezionare "Other New Records... (Altri nuovi record...)"
    - In **Select a resource record type: (Selezionare tipo di record di risorsa:)** selezionare **Service Location (Posizione servizio) (SRV)** quindi selezionare **Create Record (Crea record)**.
    - Per **Service (Servizio)** immettere: _uniteservice
    - Per **Protocol (Protocollo)** immettere: _tcp
    - Per **Port (Porta)** immettere: 443
    - Per l'host che fornisce il servizio: immettere il nome host o l'indirizzo IP dei server Enterprise.



NOTA: accedere al seguente collegamento Microsoft per conoscere i dettagli sulla configurazione di un server DNS per utilizzare le unità di inoltro feedback: https://technet.microsoft.com/en-us/library/cc754941.aspx

Appendice B. Esempio di ServerConfig.xml

Il file ServerConfig.xml viene creato durante l'installazione dei componenti hub e client del software Intel Unite. La posizione predefinita del file xml è C:\Program Files (x86)\Intel\Intel Unite\Hub o C:\Program Files (x86)\Intel\Intel Unite\Client, rispettivamente per l'hub e per il client.
Il file viene modificato quando si sceglie l'opzione **Specifica il server** e si inserisce il nome host del server, oppure quando si inserisce manualmente la **Chiave pubblica** durante l'installazione del software Intel Unite sull'hub o sul client.
Se si desidera modificare il file serverconfig.xml dopo l'installazione, accedere alla cartella nel quale risiede e apportare le modifiche necessarie.



Se un server è definito nel file ServerConfig.xml, questo avrà precedenza sul record del servizio DNS.

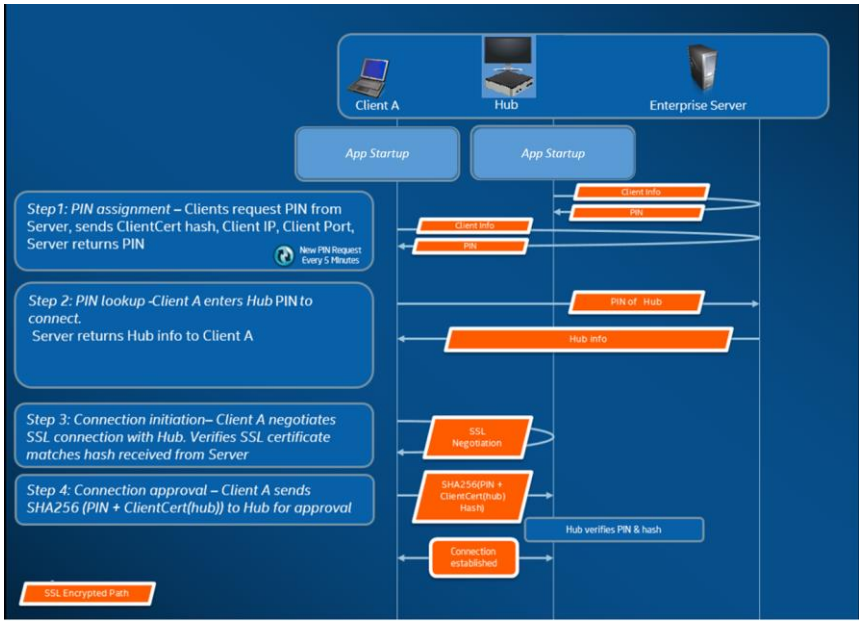
Appendice C. Soluzione Intel Unite – Panoramica sulla sicurezza

Software Intel Unite - Flusso di sicurezza

In questa sezione vengono descritti brevemente tutti gli aspetti relativi alla sicurezza dell'applicazione Intel Unite. Gli aspetti relativi alla sicurezza della connessione riguardano quattro passaggi:

1. Assegnazione PIN
2. Ricerca PIN
3. Iniziazione della connessione
4. Approvazione della connessione

La seguente immagine raffigura una panoramica di alto livello sul processo con il quale le applicazioni dell'hub e il client, dotato di tecnologia Intel vPro, ricevono PIN dal server Enterprise, li risolvono e stabiliscono una connessione.



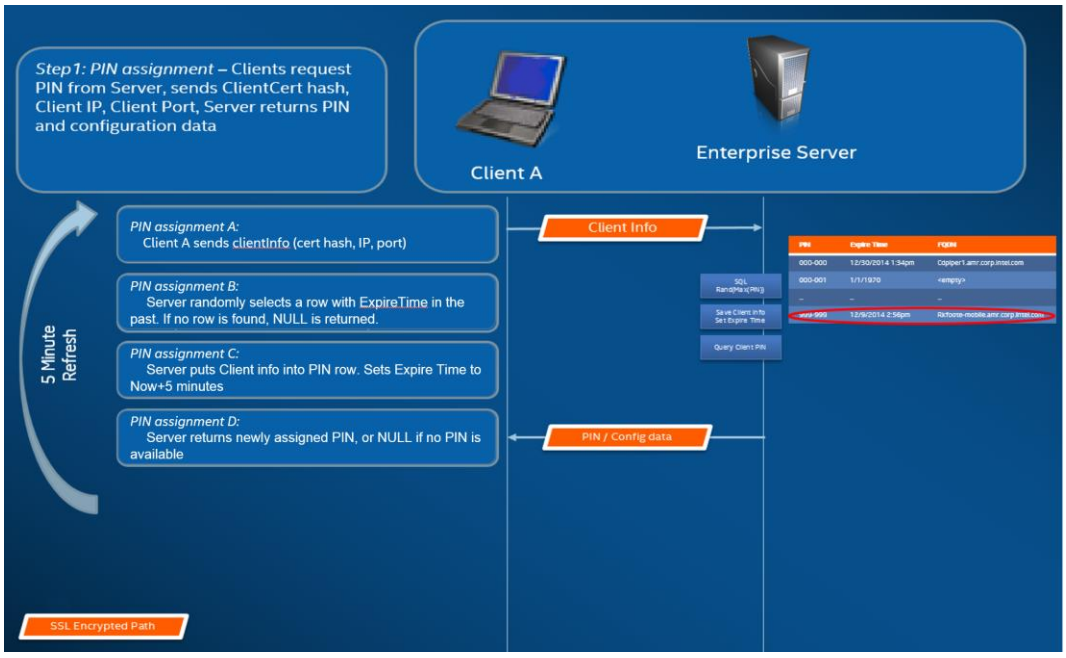
Passaggio 1: assegnazione dei PIN

La figura seguente mostra la modalità di assegnazione dei PIN. Tutte le comunicazioni dirette durante questo processo sono crittografate con SSL tramite un servizio Web (TCP 443).
Oltre a ricevere i PIN, l'hub e il client registrano anche le proprie informazioni di connessione e una chiave pubblica nel server. La chiave pubblica viene utilizzata durante la connessione, per verificare che ciascun componente comunichi con il destinatario previsto.

Nota: l'assegnazione dei PIN per client (con tecnologia Intel vPro) e hub segue lo stesso flusso.

Notare anche quanto segue:

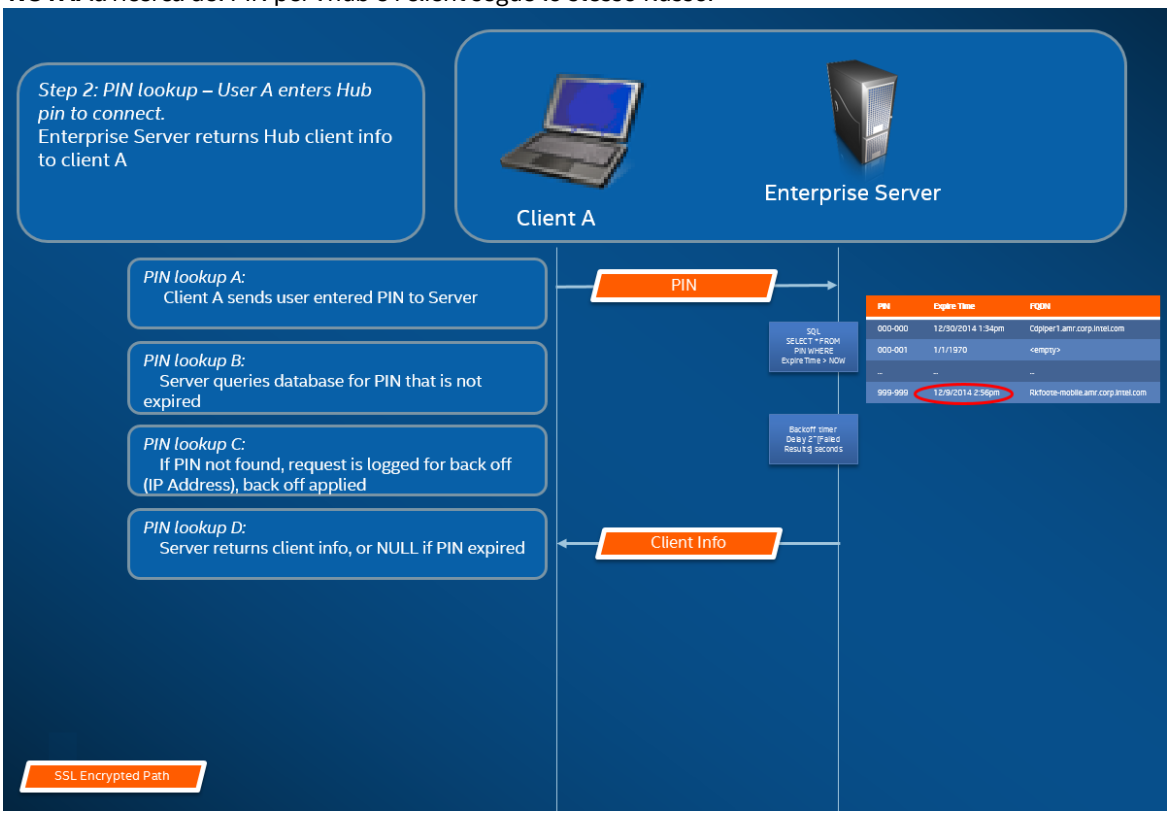
- L'intervallo di aggiornamento dei PIN è configurabile.
- Quando l'hub o il client invia le informazioni di connessione, gli indirizzi IP negli intervalli dell'host locale (127.0.0.0/8 e 169.254.0.0/16) vengono ignorati.
- La porta TCP può essere configurata a livello di client o hub. In alternativa, è possibile eseguirne il push tramite un profilo dal portale Web di amministrazione. Per impostazione predefinita, l'assegnazione della porta viene eseguita dal sistema operativo.
- I PIN scaduti possono effettuare l'accesso per un massimo di 15 secondi.
- I PIN scaduti non verranno riassegnati per un massimo di 5 minuti dopo la scadenza, per evitare che gli utenti si connettano accidentalmente al display sbagliato.



Passaggio 2: ricerca dei PIN

L'immagine qui in basso mostra la modalità con cui i PIN vengono risolti dal server Enterprise. Tutte le comunicazioni dirette durante la ricerca dei PIN sono crittografate con SSL tramite un servizio Web (TCP 443).
Quando un utente immette il PIN del dispositivo di destinazione nel client, quest'ultimo invia tale PIN al server Enterprise, che ottiene informazioni di connessione. Se la ricerca riesce, il server Enterprise restituisce informazioni di connessione valide per la destinazione. La destinazione può essere costituita da un hub o da un client (con tecnologia Intel vPro) che esegue il software Intel Unite.
Oltre a ricevere le informazioni di connessione, viene fornita anche la chiave pubblica della destinazione, cosicchè l'applicazione client può verificare che comunichi con la destinazione corretta.

NOTA: la ricerca del PIN per l'hub e i client segue lo stesso flusso.

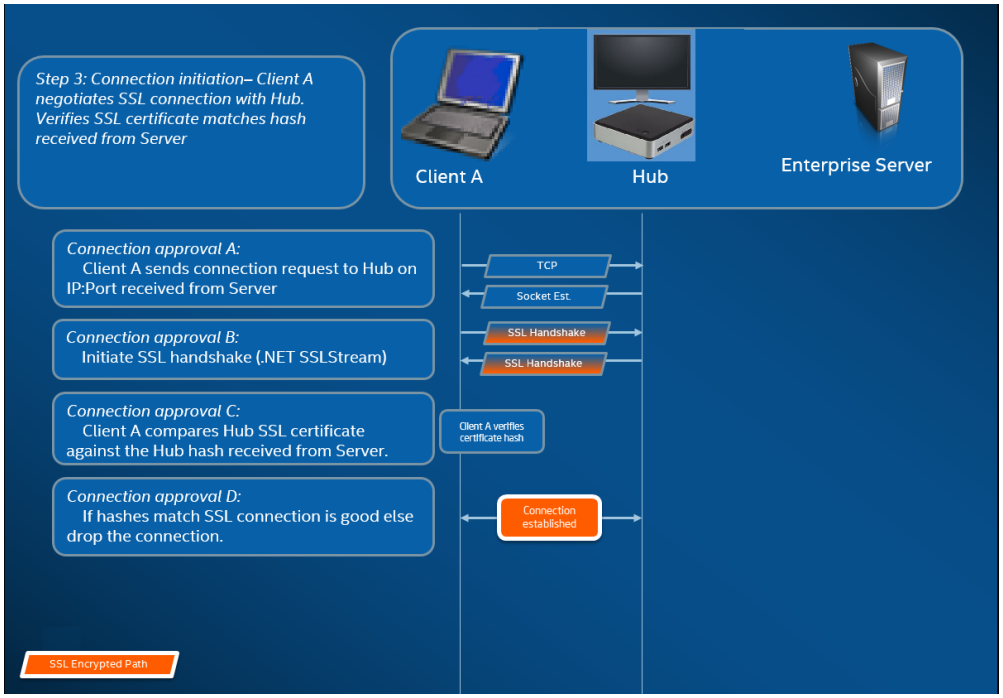


Back off della ricerca dei PIN

Per evitare che utenti malintenzionati cerchino di recuperare i PIN dal server Enterprise, i tentativi non riusciti vengono registrati. Ogni utente può effettuare fino a 3 tentativi non riusciti nell'arco di 10 secondi, dopo i quali viene attivato un meccanismo di back off che applica un ritardo di risposta (2^x secondi, dove x=numero di tentativi non riusciti in un periodo di 5 minuti).

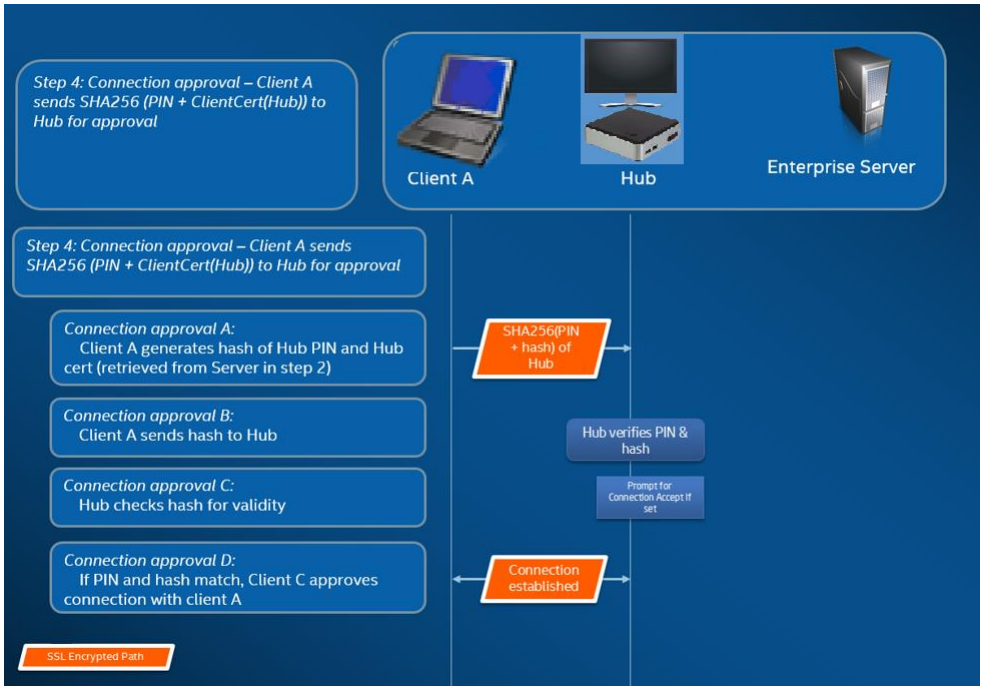
Passaggio 3: instaurazione della connessione

La figura seguente mostra l'instaurazione della connessione. In questa fase, il client stabilisce una connessione TCP peer-to-peer con la destinazione (un hub o un client con tecnologia Intel vPro che esegue il software Intel Unite) e avvia un handshake SSL. Viene calcolato l'hash del certificato fornito dalla destinazione, che viene confrontato con l'hash del client ricevuto durante il passaggio 2. Questo tipo di convalida impedisce gli attacchi ed evita anche situazioni che possono determinare una modifica degli indirizzi IP dei client DHCP.



Passaggio 4: approvazione della connessione

L'immagine riportata di seguito mostra in che modo viene stabilita la connessione tra il client e la destinazione, che potrebbe essere un hub o un client (con tecnologia Intel vPro) su cui è in esecuzione il software Intel Unite. Dopo che la destinazione ha verificato il certificato del client e il PIN, viene accettata e stabilita la connessione con il client.



Appendice D. Soluzione Intel Unite - Sistema di bilanciamento del carico

Questa sezione descrive brevemente come ovviare al backoff del PIN dietro un sistema di bilanciamento del carico/proxy.
Se si è dietro un sistema di bilanciamento del carico, è importante verificare che la stored procedure SQL dbo.spGetPinBackoffTime **restituisca sempre 0.**
Passaggi:

- Modificare la stored procedure dbo.spGetPinBackoffTime. È possibile impostare tutto come commento e utilizzare "Seleziona 0" alla fine.
- Eseguire lo script.

Se non si è dietro un sistema di bilanciamento del carico, è importante verificare che la stored procedure resti quella predefinita.