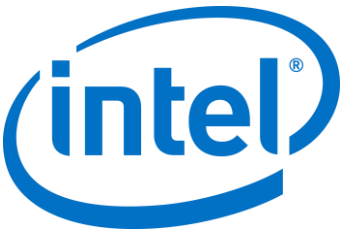
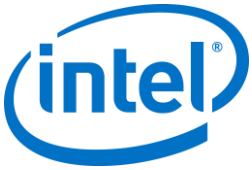


Intel Unite® Lösung

Installationsleitfaden für Unternehmen

Mai 2017



Haftungsausschluss und Urheberrechte

Die hier angegebenen Informationen sind freibleibend. Wenden Sie sich an Ihren Intel Vertreter, um die neuesten Produktspezifikationen und Pläne von Intel zu erhalten.

Die Funktionsmerkmale und Vorteile von Intel Technik hängen von der Systemkonfiguration ab und können geeignete Hardware, Software oder die Aktivierung von Diensten erfordern. Die Leistungsmerkmale variieren je nach Systemkonfiguration. Kein Computersystem bietet absolute Sicherheit. Informieren Sie sich beim Systemhersteller oder Einzelhändler oder unter intel.com.

Sie dürfen dieses Dokument nicht in Verbindung mit einer Rechtsverletzung oder anderen rechtlichen Überprüfung in Hinblick auf hier beschriebene Intel Produkte verwenden noch dessen Verwendung Dritten ermöglichen. Sie stimmen zu, Intel eine einfache, gebührenfreie Lizenz auf jeglichen Patentanspruch, der zu einem späteren Zeitpunkt aufgesetzt wird und hier behandelte Themen umfasst, zu gewähren.

Durch dieses Dokument werden (weder ausdrücklich noch konkludent oder auf andere Weise) irgendwelche Rechte an geistigem Eigentum gewährt.

Die in diesem Dokument beschriebenen Produkte können konstruktionsbedingte Defekte oder Fehler (Errata) enthalten, die zu Abweichungen der Produkteigenschaften von den angegebenen Spezifikationen führen. Eine Liste derzeit bekannter Errata ist auf Anfrage verfügbar.

Intel lehnt alle ausdrücklichen und stillschweigenden Garantien ab, insbesondere (aber nicht beschränkt auf) die stillschweigenden Garantien für die Marktgängigkeit, die Eignung für einen bestimmten Zweck und die Nichtverletzung von Urheberrechten, sowie sämtliche Garantien, die sich aus der Art und Weise der Vertragserfüllung oder dem Handelsbruch ergeben.

Intel hat keinen Einfluss auf und keine Aufsicht über die Benchmarkdaten Dritter oder die Websites, auf die in diesem Dokument Bezug genommen wird. Besuchen Sie die genannten Websites, um sich davon zu überzeugen, dass die angeführten Benchmarkdaten zutreffen.

Intel, das Intel Logo, Intel Unite, Intel Core und Intel vPro sind Marken der Intel Corporation oder ihrer Tochtergesellschaften in den USA und/oder anderen Ländern.

Einige der Abbildungen in diesem Dokument werden möglicherweise aufgrund der Lokalisation anders dargestellt.

*Andere Marken oder Produktnamen sind Eigentum der jeweiligen Inhaber.

Inhaltsverzeichnis

1 Einleitung

Die Intel Unite® Software bringt sichere, miteinander verbundene Meetingräume zur Vereinfachung der Zusammenarbeit. Mit der Software können sich die Teilnehmer eines Meetings schnell und einfach verbinden. Die Intel Unite Lösung ermöglicht bereits heute eine einfache und sofortige Zusammenarbeit und bildet die Grundlage für weitere Funktionen und Innovationen in der Zukunft.
Dieses Dokument kann bei der Installation der Intel Unite Software im Unternehmensmodus verwendet werden und stellt Informationen zu den Funktionen sowie Unterstützung bei der Fehlerbehebung bereit.

1.1 Publikum

Dieses Dokument richtet sich an IT-Spezialisten sowie an andere Zielgruppen, die die Intel Unite Lösung in einem Unternehmensumfeld einsetzen.

1.2 Intel Unite Lösung – Begriffe und Definitionen

Enterprise-Server (Server) – Dieser Begriff bezieht sich auf den Webserver und den PIN-Dienst, der auf dem Server ausgeführt wird, um PINs zuzuweisen und aufzulösen. Er bietet eine Download-Seite für die Clients und das Admin-Portal zur Konfiguration.

Client – Dieser Begriff bezeichnet ein Gerät (Windows*, macOS*, iOS*, Android* oder Chromebook*), das verwendet wird, um sich mit dem Hub zu verbinden.

Hub – Dieser Begriff bezeichnet einen PC im Mini-Format mit Intel® vPro™ Technologie, der mit einem Display im Konferenzraum verbunden ist und auf dem die Intel Unite Anwendung ausgeführt wird.

FQDN – Dieses Akronym steht für „Fully Qualified Domain Name“ (vollqualifizierter Domänenname).

Plugin – Dieser Begriff bezeichnet eine Software-Komponente, die auf dem Hub installiert ist und mit der die Funktionalität der Intel Unite Lösung erweitert wird.

IIS – Dieses Akronym steht für „Internet Information Services“ (Internetinformationsdienste), ein von Microsoft* bereitgestellter Webserver.

1.3 Was ist neu an der Intel Unite Lösung

Damit Sie einfacher überblicken können, was neu an der Lösung ist, werden in der folgenden Tabelle die Funktionen aufgelistet, die seit Version 1.0 hinzugefügt wurden.

v 2.0	v 3.0	v 3.0 MR	v 3.1
Erweiterter Bildschirm	Audio-/Video-Streaming mit Hardware-Beschleunigung für Windows (1080 bei 20-30 fps)	iOS-Support bis zur aktuellen Version	Mehr Benutzerkomfort beim Admin-Portal, ein anderes Aussehen einschließlich hinzugefügter Dialogfelder zur leichteren Auswahl der Einstellungen
Support von Windows 10	Plugin für geschützten Gastzugang		Admin-Portal: Meeting planen
Plugin für Gast-Login	Geplante Meetings (Einzelzimmer)		Admin-Portal: Moderatormodus
Plugin für Skype for Business	Meeting-Sperre		Admin-Portal: Statische PIN
	iOS-Support zur Ansicht		Admin-Portal: PIN-Reservierung
			Admin-Portal: PIN-Transparenz
			Admin-Portal: Deaktivieren der Remote-Ansicht
			Chrome OS-Unterstützung
			Android-Unterstützung

2 Intel Unite Lösung – Anforderungen

2.1 Enterprise-Server – Anforderungen

- Microsoft Windows* Server 2008 und neuer
- Microsoft Internet Information Services, SSL-aktiviert
    - SHA2-basiertes Webserverzertifikat mit interner oder öffentlicher Vertrauensstellung erforderlich
- Unter Microsoft Internet Information Services konfigurierter SMTP-E-Mail-Server
- Microsoft SQL Server2008 R2 oder neuer
- Microsoft .NET* 4.5 oder neuer
- 4 GB RAM
- 32 GB verfügbarer Speicher
  HINWEIS: Der IIS-Webserver und Microsoft SQL-Datenbankserver können auf unterschiedlichen Computern installiert werden.

2.2 Hub-Anforderungen

- Microsoft Windows 7 SP1, 8.1 oder 10 (32-Bit und 64-Bit)
    - Empfohlener neuester Patch-Level
- Microsoft .NET 4,5 und neuer
- Unterstützter SKU[1], Mini-PC mit Intel® Core™ vPro™ Prozessor der 4. Generation oder neuer
- Verdrahtete oder Funk-Netzwerkverbindung
- 4 GB RAM
- 32 GB verfügbarer Speicher

2.3 Client-Anforderungen

- Microsoft Windows 7 SP1, 8.1 oder 10 (32-Bit und 64-Bit)
    - Empfohlener neuester Patch-Level
- Microsoft .NET 4,5 und neuer
- OS X* 10.10.5 und neuer
- iOS 9.3 oder höher
- Verdrahtete oder Funk-Netzwerkverbindung

[1] Wenden Sie sich für unterstützte SKUs an Ihren bevorzugten OEM oder Ihren Ansprechpartner bei Intel

2.4 IT-Faktoren und Netzwerkanforderungen

Verwenden Sie zur Installation des Hubs und Clients die in Ihrer IT-Abteilung etablierten Prozesse zur Softwareverteilung.
Wir empfehlen für den Hub dringend die Verwendung einer kabelgebundenen Netzwerkverbindung. Dadurch wird besonders in Ballungsräumen eine Sättigung der Drahtlosfrequenz vermieden.
Beachten Sie außerdem, dass die Intel Unite Software so eingestellt werden muss, dass eingehende Verbindungen angenommen werden. Eventuell müssen Sie der auf dem Hub installierten Firewall eine Ausnahme hinzufügen. Informationen zum Erstellen von Anwendungsausnahmen erhalten Sie bei Ihrem Firewallanbieter.

Für eine Produktionsumgebung empfehlen wir dringend die Verwendung eines vollqualifizierten Domänennamens (Fully Qualified Domain Name, FQDN) und die Einrichtung eines DNS-Diensteintrags, der auf den Enterprise-Server verweist. Dies ist für Hubs und Clients die einfachste Methode, um den Enterprise-Server zu suchen.
Als Sicherheits-Upgrade akzeptiert die Anwendung nur SHA-2 oder höhere Zertifikate. Dies kann es erforderlich machen, dass Sie die Zertifikate auf Ihrem Webserver upgraden. Arbeiten Sie mit Ihrem IT-Sicherheitsteam, um SHA-2-Zertifikate während der Installation zu erhalten.

2.4.1 Mobile Client-Geräte

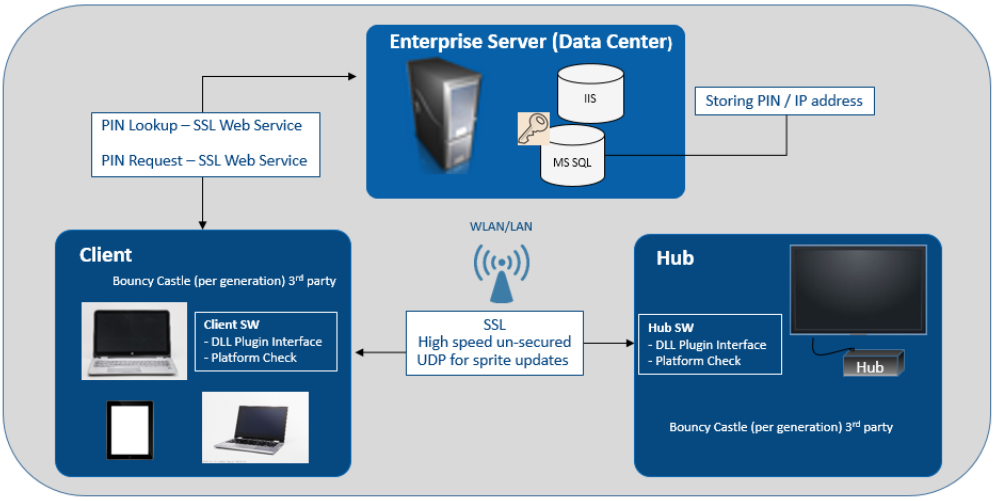
Wenn Ihr Unternehmen künftig mobile Client-Geräte als Teil des Intel Unite Client-Betriebssystems bereitstellt, sollten Sie Folgendes beachten:
Alle Client-Geräte müssen mit dem Unternehmensnetzwerk verbunden sein oder ein entsprechend konfiguriertes VPN verwenden. Das betrifft sowohl iOS- als auch Android-Geräte. Bei dem Versuch, eine Verbindung mit der Intel® Unite™ App über ein normalerweise privat genutztes Tablet oder Mobiltelefon herzustellen, können Probleme auftreten, wenn das Tablet oder Mobiltelefon nicht über das Unternehmensnetzwerk, sondern über einen eigenen Mobilfunkanbieter verbunden ist, da die Firewall des Unternehmens diese Verbindung möglicherweise nicht zulässt.

Für IT-Administratoren:

- Verwendet ein Benutzer die Intel® Unite™ App über sein privates Mobilgerät, müssen Sie sicherstellen, dass dieses Gerät im Unternehmensnetzwerk die Berechtigung für den Zugriff auf Intel Unite hat oder dass die Verbindung auf einem anderen Weg zustande kommt.
- Stellen Sie sicher, dass Ihnen alle erforderlichen Tools für die Verwaltung dieser Geräte und für die Sicherheit des Netzwerks zur Verfügung stehen.
- Für die Verwaltung dieser Geräte, die ein zusätzliches Sicherheitsrisiko darstellen können, wird eine richtige Strategie benötigt.
- Richten Sie eine Mobile-Device-Management-Lösung für Mobilgeräte ein, sowohl für Geräte für den privaten als auch den geschäftlichen Gebrauch.
- Maßgeschneiderte Sicherheitsfunktionen helfen dabei, das richtige Maß an Sicherheit in Abhängigkeit von der Sensibilität der Daten bereitzustellen. Der Anpassungsgrad steht in direkter Relation zu den Daten, die für Ihr Unternehmen von entscheidender Bedeutung sind, und wie weit Sie für diesen Schutz gewillt sind zu gehen.

3 Bereitstellung im Überblick

Die Intel Unite Lösung besteht aus drei Komponenten – einem Enterprise-Server, einem Hub und einem Client.
Als erstes müssen Sie den Enterprise-Server einrichten. Die gestarteten Hub- und Client-Anwendungen greifen auf den Enterprise-Server zu, um Verbindungsinformationen und PIN-Zuweisungen auszutauschen.
Beim Hub handelt es sich um einen Mini-PC mit Intel Core vPro Prozessor, der üblicherweise mit einem Bildschirm oder Projektor in einem Konferenzraum verbunden ist.
Clients führen die auf dem Hub angezeigten Anweisungen aus, um die Clientsoftware herunterzuladen und sich mit dem Hub durch Eingabe der angezeigten PIN zu verbinden. Sobald die Verbindung besteht, kann ein Client Inhalte präsentieren, anzeigen und beschriften sowie Dateien mit anderen Teilnehmern teilen, die mit demselben Hub verbunden sind, und mit auf dem Hub installierten Plugins interagieren.
In diesem Diagramm wird ein Überblick über die installierten Komponenten bereitgestellt.



3.1 Bereitstellungsressourcen

Zum Abschluss der Installation benötigen Sie Folgendes:

- Administratorrechte auf die Datenbank
- Administratorrechte auf den Enterprise-Server
- Administratorrechte auf den Hub

Eventuell benötigen Sie außerdem Folgendes:

- IT-Sicherheitsadministrator, um das SHA2-Zertifikat auszustellen
- IT-Sicherheitsadministrator für Firewall-Richtlinien
- IT-Administrator zum Erstellen eines DNS-Diensteintrags zur Verwendung von Hub und Clients für die Suche nach dem Enterprise-Server (dringend empfohlen)

4 Enterprise-Server Installation

4.1 Der Enterprise-Server im Überblick

Das Enterprise-Server-Installationsprogramm beinhaltet die Datenbank, den PIN-Server, das Admin-Webportal und die Downloadseite für den Client.
Der Enterprise-Server umfasst 4 Komponenten:

1) Microsoft SQL-Datenbank: Verwaltet alle Statusinformationen für die Infrastruktur der Intel Unite Lösung.
2) Webdienst: Ein standardisierter Mitteilungsdienst, der mit der Datenbank und den Hubs und Clients kommuniziert.
3) Admin-Portal: Verwaltet Hubs und Clients, erstellt Statistiken, überwacht und gibt Warnmeldungen aus.
4) Download-Angebotsseite für den Client: Hier ist die Intel Unite Software für den Client enthalten.

Außerdem ist es wichtig zu wissen, dass die Hubs und Clients den Enterprise-Server über die folgenden zwei Methoden in der Netzwerkinfrastruktur suchen: über die Datei „ServerConfig.xml“ oder den DNS-Diensteintrag.
Wir empfehlen die Verwendung des DNS-Diensteintrags, da dies die Zero-Touch-Konfiguration des Clients und Hubs ermöglicht. Siehe Abschnitt Erstellen eines DNS-Diensteintrags. Wenn Sie jedoch keinen DNS-Diensteintrag erwerben können, kann der Enterprise-Server in der Datei „ServerConfig.xml“ konfiguriert werden. Siehe Anhang B für ein Beispiel einer ServerConfig.xml-Datei.

4.2 Vor der Installation des Enterprise-Servers

- Stellen Sie sicher, dass der Server die angegebenen Mindestanforderungen für die Software und Hardware erfüllt.
- Stellen Sie sicher, dass die Internet Information Services (IIS)-Version 8.0 oder neuer auf Ihrem Server installiert ist. Das Server-Installationsprogramm erfordert die Aktivierung von IIS, um Fehler bei der Installation zu vermeiden. Informationen zur Aktivierung und Einstellung des IIS finden Sie im Abschnitt zu Aktivieren von IIS.
- Richten Sie den SMTP-E-Mail-Server im IIS-Manager ein, siehe Abschnitt
- E-Mail-Server-Einstellungen.
- ASP.NET 4.5 muss installiert und aktiviert sein.
- Stellen Sie sicher, dass SSL in IIS (HTTP-Websites müssen funktionieren) aktiviert ist. **HINWEIS:** Eventuell müssen Sie zur Installation eines SHA-2 Zertifikats mit gültiger Stammvertrauensstellung mit Ihrer IT-Abteilung zusammenarbeiten.
- Stellen Sie sicher, dass Sie über Administratorrechte verfügen, um über die Windows- oder SQL-Authentifizierung auf MS SQL zuzugreifen, siehe Abschnitt Microsoft SQL Server installieren.
- Fügen Sie einen DNS-Diensteintrag hinzu, um eine automatische Suche nach dem Enterprise-Server zu ermöglichen. Siehe Abschnitt Erstellen eines DNS-Diensteintrags.

4.2.1 Software-Upgrade

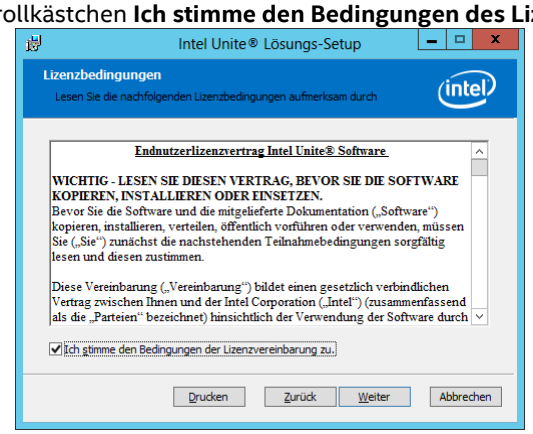
Wenn Ihr Unternehmen ein Software-Upgrade durchführt:

- Erstellen Sie unbedingt ein Backup der Datenbank, da Änderungen nicht mehr rückgängig gemacht werden können.
- Alle Verbindungen zur Datenbank müssen vor dem Upgrade geschlossen sein (Abmelden vom Admin-Portal)
- Während des Upgrades ist die Datenbank-Option standardmäßig ausgewählt, sowohl zur lokalen als auch zur Remote-Installation, wenn Intel Unite Server.msi auf dem PIN-Server ausgeführt wird.

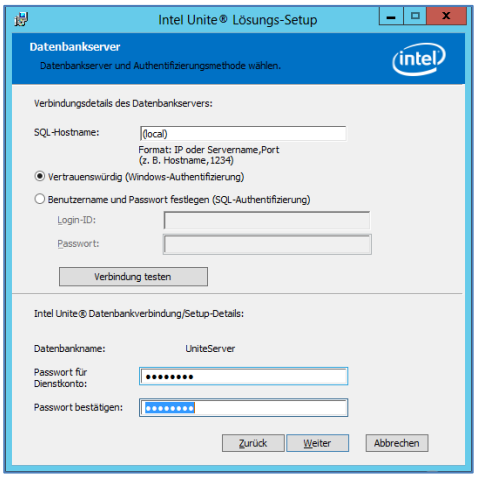
4.3 Enterprise-Server Installation

Sobald Sie alle Schritte im vorherigen Abschnitt (Vor der Installation des Enterprise-Servers) überprüft haben, können Sie mit den Intel Unite Software-Installationsprogrammen fortfahren (dieser Prozess muss auf dem Server ausgeführt werden, der die IIS-Umgebung hostet).

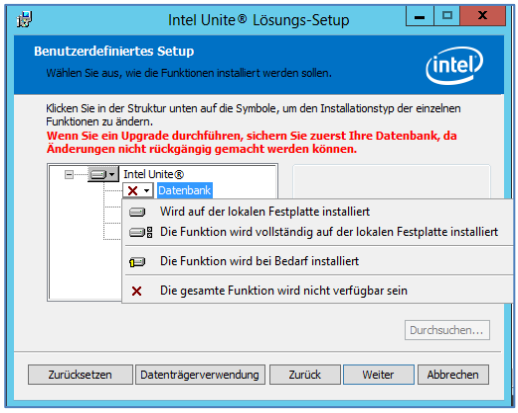
- Suchen Sie nach der Datei **Intel Unite Server.mui.msi** und doppelklicken Sie darauf, um sie auf dem oder den Zielservern zu installieren.
- Der Installationsassistent schlägt die Installation folgender Komponenten vor: Datenbank, Webdienst, Client-Downloadseite und Admin-Portal.
- Akzeptieren Sie, nachdem **Intel Unite Server.mui.msi** gestartet wurde, die Lizenzvereinbarung, indem Sie das Kontrollkästchen **Ich stimme den Bedingungen des Lizenzvertrags zu** aktivieren.

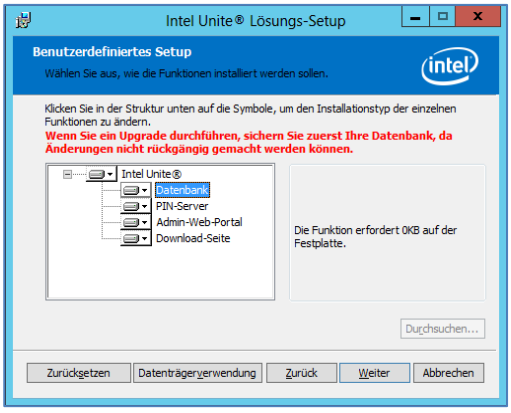


- Klicken Sie auf **Weiter**, um das Fenster „Datenbankserver" zu öffnen.
- Wählen Sie im Fenster „Datenbankserver" die Option **Details zur Datenbankserver-Verbindung** aus. Folgende Optionen sind verfügbar:
  - Im Feld **SQL Hostname** ist für den SQL Server **(local)** als Standardwert angegeben. Sie können den Wert durch die Bearbeitung des Hostnamens ändern oder den Standardwert beibehalten (behalten Sie **(local)** bei, wenn SQL auf demselben Server installiert ist).
  - Der Standardwert für den Server ist **Vertrauenswürdig (Windows-Authentifizierung)**, (wenn Sie bereits angemeldet sind). Wählen Sie ansonsten **Benutzername und Passwort festlegen (SQL-Authentifizierung)**, wenn Sie gültige Anmeldeinformationen für den Zugriff auf die Datenbank haben und die SQL-Authentifizierung bevorzugen. Wenn Sie sich für die zweite Option entscheiden, achten Sie darauf, dass Sie die Datenbank TESTEN, indem Sie auf **Verbindung testen**.
  - Sie müssen im Abschnitt **Intel Unite Datenbankverbindung/Setup-Details** ein Passwort für **UniteServiceUser** erstellen, das für den Zugriff auf die neue Datenbank namens UniteServer verwendet wird. **Bestätigen Sie das Passwort** im nächsten Feld.
  - Das Passwort muss aus mindestens 8 Zeichen bestehen, darunter mindestens ein Großbuchstabe, ein Kleinbuchstabe, eine Zahl und ein Symbol.



- Klicken Sie auf **Weiter**, um das Fenster **Benutzerdefiniertes Setup** für die Auswahl der Funktionen zu öffnen. Erweitern Sie die Datenbankfunktion und wählen Sie **Wird auf der lokalen Festplatte installiert** oder **Die Funktion wird vollständig auf der lokalen Festplatte installiert**. So wird die Datenbank auf dem SQL Server erstellt, der im vorigen Schritt eingerichtet wurde.

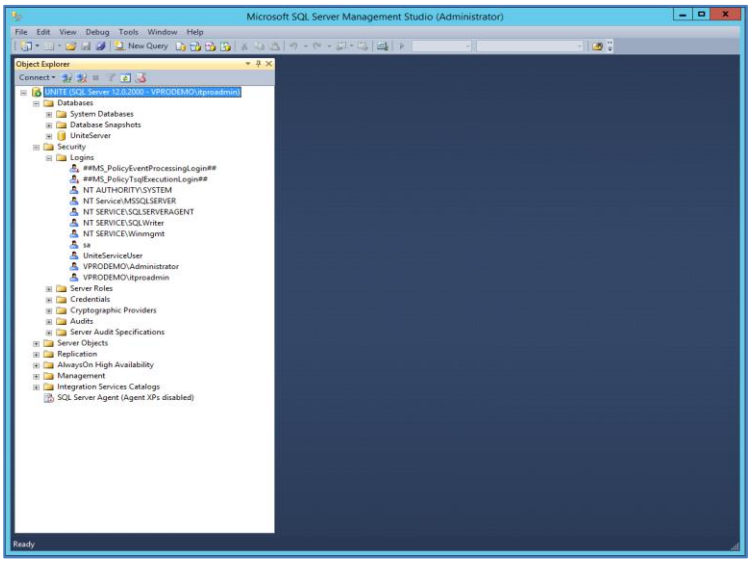




- Klicken Sie auf **Weiter**, um die Auswahl der Funktion zu prüfen, und klicken Sie zum Starten der Installation auf **Installieren**.
- Klicken Sie auf **Fertig stellen**, um die Installation abzuschließen.
- Enterprise-Server ist jetzt installiert. Fahren Sie mit dem nächsten Abschnitt fort, um den Hub zu installieren.

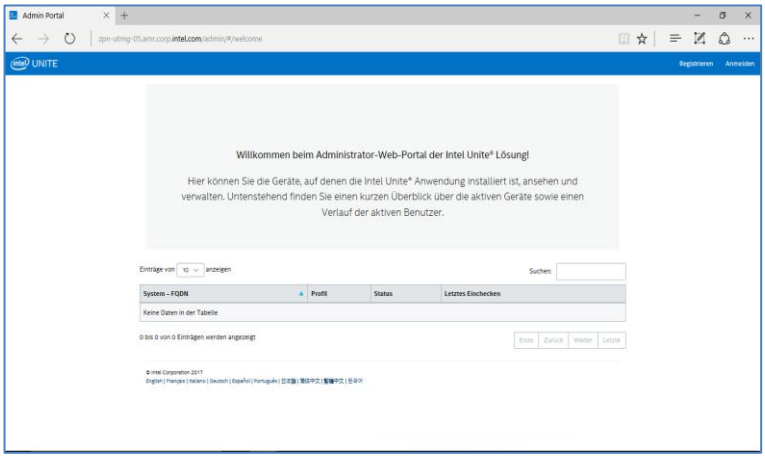
Optional:

- Wenn Sie überprüfen wollen, ob die UniteServer-Datenbank mit SQL Management Studio erstellt wurde, öffnen Sie SQL Management Studio auf Ihrem Server und stellen Sie eine Verbindung zum SQL-Server her. Erweitern Sie die Datenbanken im linken Bereich und prüfen Sie, ob die UniteServer-Datenbank erstellt wurde.



- Überprüfen Sie, ob die Installation erfolgreich abgeschlossen wurde, indem Sie über den folgenden Link auf das Admin-Portal (bei Installation mit der Datenbank und dem PIN-Server auf dem Server):
  https://<yourservername>/admin

  Melden Sie sich bei Ihrem Konto an oder verwenden Sie das standardmäßige Administratorkonto (für die Neuinstallation von Software):
  Benutzer: admin@server.com
  Passwort: Admin@1

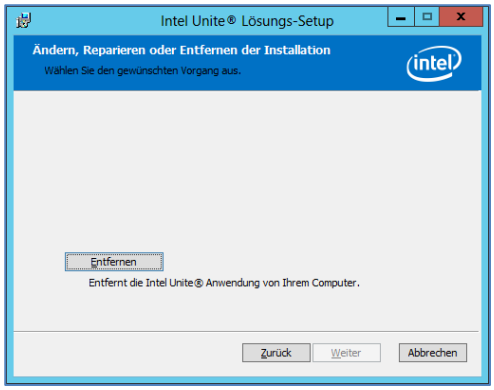


Hinweis: Wenn beim Zugriff auf das Admin-Portal eine Fehlermeldung erscheint, siehe Abschnitt Fehlerbehebung.

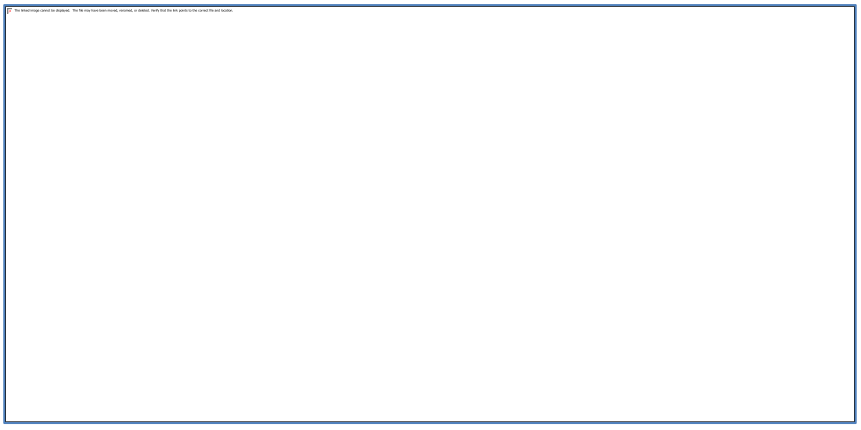
4.4 Deinstallieren der Intel Unite Anwendung

Wenn die Anwendung deinstalliert werden muss, müssen Sie auch die zuvor erstellte UniteServer-Datenbank und den UniteServiceUser-Login löschen, um Konflikte innerhalb der Anwendung zu vermeiden. Bevor Sie dies tun, **stellen Sie sicher, dass Sie ein Backup Ihrer Datenbank erstellt haben**.

1. Starten Sie das Installationsprogramm **Intel Unite Server.mui**.
2. Klicken Sie auf **Entfernen** und **Weiter**, um fortzufahren.



3. Gehen Sie zum Microsoft SQL Server Management Studio und löschen Sie manuell die **UniteServer** SQL-Datenbank und das **UniteServiceUser**-Konto. Siehe hervorgehobene Bereiche im Bild oben.



5 Installation des Hubs

5.1 Vor der Installation des Hubs

Die Intel Unite Anwendung benötigt eine Ausnahme in der Hub-Firewall, um mit dem Enterprise-Server kommunizieren und bei ihm einchecken zu können, da der Hub den Enterprise-Server lokalisieren und bei ihm einchecken können muss.

Wenn Sie das Hub-Installationsprogramm ausführen, werden Sie zur Eingabe der Server-Verbindungsdaten aufgefordert. Außerdem haben Sie die Möglichkeit, die manuelle Suche (die Option **Server festlegen** im Installationsprozess) zu umgehen und stattdessen die Informationen aus dem DNS-Diensteintrag zu übernehmen. Wenn das Hub-Installationsprogramm ausgeführt wird, wird die Datei „ServerConfig.xml“ bearbeitet.

Je nach gewählter Methode für PIN-Lookup müssen Sie wissen, ob Sie **Automatische Suche nach Server** oder **Server festlegen** während der Installation auswählen werden.

Wenn Sie wissen, dass der DNS-Diensteintrag existiert, können Sie Automatische Suche nach Server auswählen, wenn Sie nicht sicher sind, verwenden Sie die Option Server festlegen (manuelle Suche). Bei dieser Option müssen Sie den Hostnamen für den Enterprise-Server kennen.

Wenn Sie die Datei „ServerConfig.xml“ mit dem öffentlichen Schlüssel (siehe nächsten Abschnitt Öffentlicher Schlüssel) bearbeitet haben, ist die erneute Eingabe des Schlüssels für die Client- und Hub-Installationsprogramme nicht erforderlich.

Hinweis: Wenn in der Datei „ServerConfig.xml“ ein Server angegeben wurde, hat dieser Vorrang vor dem DNS-Diensteintrag.

5.1.1 Öffentlicher Schlüssel

Der öffentliche Schlüssel ist optional und seine Aufgabe besteht darin, festzulegen, wie der Hub und Client mit dem Enterprise-Server kommuniziert. Wenn er nicht angegeben wird, überprüfen Hub und Client die Vertrauenswürdigkeit. Wenn die Anwendung das Zertifikat nicht akzeptiert, wird der Benutzer zur Eingabe aufgefordert.

Der öffentliche Schlüssel wird verwendet, wenn Sie die Installation von Hub und Client durchführen. Sie benötigen diesen Schlüssel zur Ausführung der Installationsprogramme von Hub und Client. Den öffentlichen Schlüssel erhalten Sie unter: https://yourservername/unite/ccservice.asmx

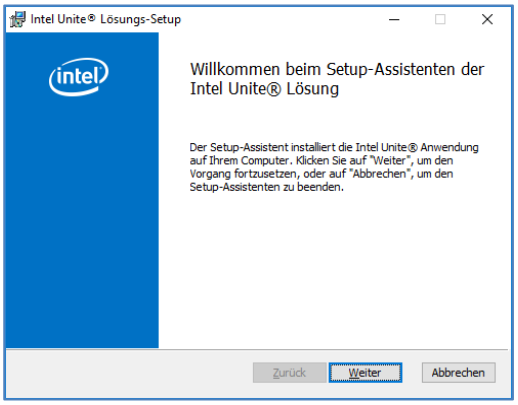
Klicken Sie in der Adresszeile auf das Schloss und sehen Sie die Zertifikatsinformationen ein. Gehen Sie zu „Details“, klicken Sie auf „Show all“, scrollen Sie im Feld nach unten zu „Public Key“, und klicken Sie dann auf den öffentlichen Schlüssel, den Sie anzeigen möchten. Sie können den Wert auch herauskopieren und ihn in die ServerConfig.xml einfügen.

Stellen Sie sicher, dass Sie die Leerzeichen nach dem Einfügen in „ServerConfig“ entfernen. Wenn Sie die Datei „ServerConfig.xml“ mit dem öffentlichen Schlüssel bearbeitet haben, muss der Schlüssel für die Client- und Hub-Installationsprogramme nicht erneut eingegeben werden. Siehe Anhang B für ein Beispiel einer ServerConfig.xml-Datei.

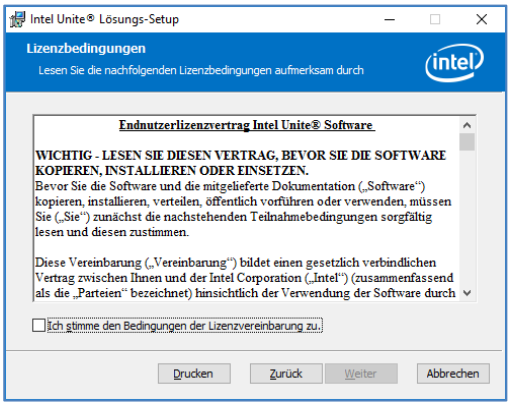
5.2 Installation des Hubs

- Suchen Sie nach dem Installationsprogrammordner und führen Sie das Installationsprogramm des Hubs aus: **Intel Unite Hub.mui.msi**

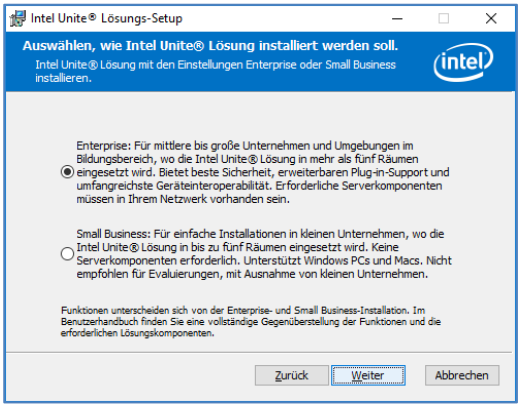
- Klicken Sie auf **Weiter**, um fortzufahren.



- Markieren Sie das Kontrollkästchen **Ich stimme den Bedingungen der Lizenzvereinbarung zu** und klicken Sie dann auf **Weiter**.

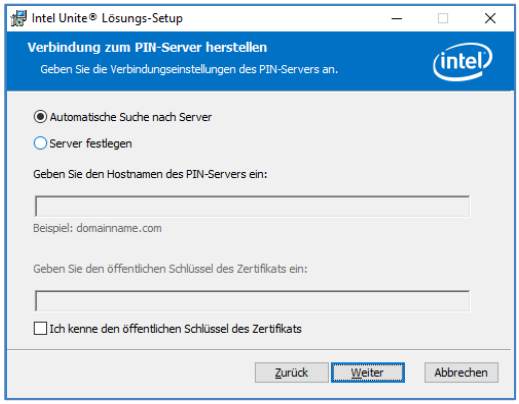


- Wählen Sie **Enterprise** aus und klicken Sie auf **Weiter**.

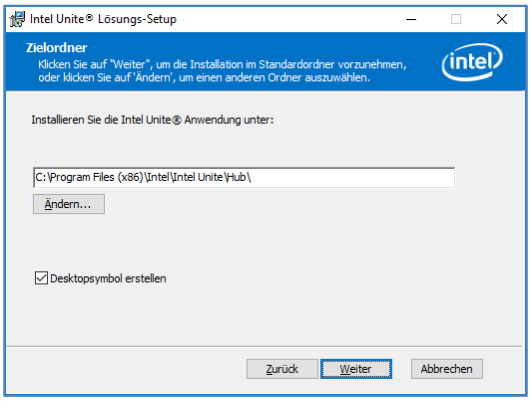


- In diesem Fenster müssen Sie die Verbindungseinstellungen für den PIN-Server angeben. Sie haben folgende Optionen zur Auswahl:
  - **Automatische Suche nach Server**: Diese Option wird empfohlen (Standard).
  - **Server festlegen**: In diesem Schritt muss Ihnen der Hostname des Enterprise-Servers bekannt sein
    - **Geben Sie den Hostnamen des PIN-Servers ein.**
    - Geben Sie den **Öffentlichen Schlüssel des Zertifikats** ein, wenn Sie das Kontrollkästchen **Ich kenne den öffentlichen Schlüssel des Zertifikats** aktiviert haben.

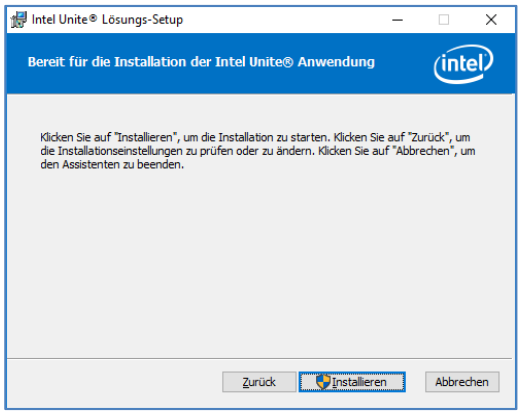
  Treffen Sie Ihre Auswahl und klicken Sie dann auf **Weiter**.



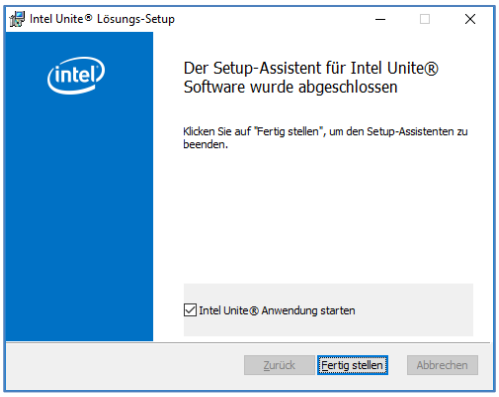
- Das Fenster **Zielordner** wird mit dem Standardordner geöffnet, in dem der Hub installiert wird. Sie können den Zielordner nach Belieben ändern oder den Standardspeicherort beibehalten. In diesem Schritt können Sie zudem ein Desktopsymbol erstellen. Klicken Sie auf **Weiter**, um fortzufahren.



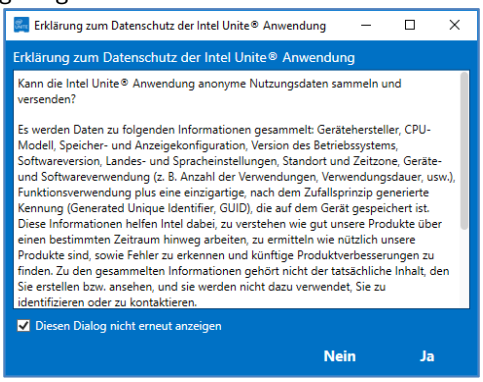
- Sie haben die Möglichkeit, zurückzugehen, um Ihre Einstellungen zu überprüfen, oder Sie können auf **Installieren** klicken, um den Vorgang fortzusetzen.



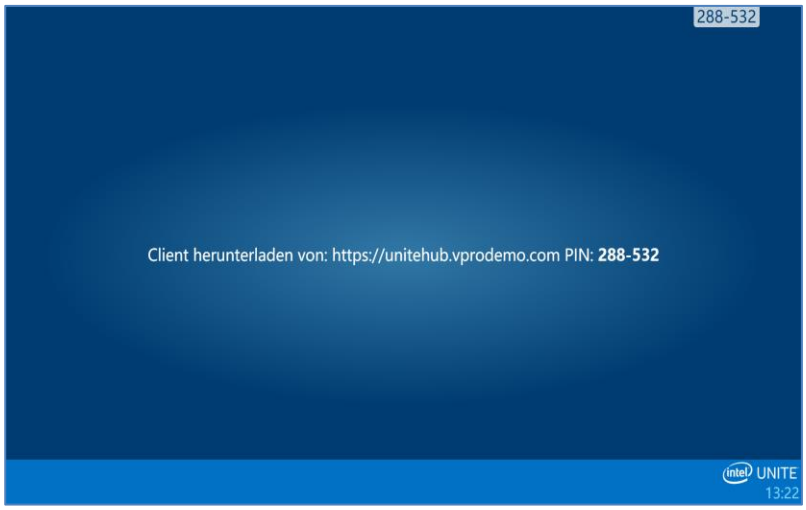
- Nach Abschluss der Installation wird Ihnen das Fenster **Der Setup-Assistent für Intel Unite® Software wurde abgeschlossen** angezeigt. Klicken Sie auf Fertigstellen, um die Installation abzuschließen.



- Wenn Sie die Anwendung zum ersten Mal starten, wird die **Datenschutzerklärung für die Intel Unite® Anwendung** angezeigt.



- Die Datenschutzerklärungsfunktion für die Intel Unite® Anwendung wird für die Erfassung anonymer Nutzungsdaten verwendet. Intel ist stets bemüht, die angebotenen Produkte zu verbessern und sammelt daher Daten für die weitere Verbesserung seiner Produkte. Wählen Sie **JA** oder **NEIN** und markieren Sie das Kästchen, wenn das Dialogfeld nicht mehr angezeigt werden soll.
- Auf Ihrem Bildschirm oder Monitor wird nun eine PIN angezeigt. Sie benötigen diese PIN, damit sich die Clients mit dem Hub verbinden können. (Siehe Abschnitt Fehlerbehebung, wenn die PIN nicht angezeigt wird.)



5.3 Konfiguration des Hubs

Für Hubs, die die Intel Unite Software ausführen, können Konfigurationsoptionen über das Admin-Portal geändert werden. Im Admin-Portal ist ein Standardprofil mit Standardkonfigurationseinstellungen enthalten, das auf alle Hubs angewendet wird, die beim Enterprise-Server einchecken. Die Konfigurationsoptionen werden an die Hubs weitergegeben, nachdem eine Verbindung vom Hub mit dem Enterprise-Server erstellt wurde. Die Einstellungen werden bei jeder Anmeldung des Hubs aktualisiert. Die meisten Einstellungen für den Hub können an die Bedürfnisse Ihres Unternehmens angepasst werden, beispielsweise kann jeder Hub in der Anzeige eine andere Farbe, ein anderes Bild oder eine andere PIN-Größe aufweisen, unterschiedliche Plugins beinhalten etc.
Weitere Informationen über die Hub-Konfiguration finden Sie im Abschnitt Leitfaden für das Admin-Portal.

5.4 Empfohlene Hub-Konfiguration

Um eine bestmögliche Benutzerfreundlichkeit zu gewährleisten, sollte der Hub so konfiguriert werden, dass er immer einsatzbereit ist und System- oder Popup-Benachrichtigungen auf dem Bildschirm unterdrückt werden. Folgende Empfehlungen werden gegeben:

- Windows muss die Domäne oder den Benutzer, die Intel Unite ausführt, automatisch anmelden
- Bildschirmschoner müssen deaktiviert sein.
- Das System darf nie in den Standby-Modus versetzt werden.
- Das System darf nie abgemeldet werden.
- Das Display darf nie ausgeschaltet werden.
- Systembenachrichtigungen müssen unterdrückt werden.

5.5 Hub-Sicherheit

Der Hub-Administrator muss sicherstellen, dass die empfohlenen Sicherheitsverfahren für jeden Hub eingehalten werden. Wenn der lokale Benutzer automatisch angemeldet wird, muss dieser ohne Administratorrechte angemeldet werden.

5.6 Plugins

Die Intel Unite Anwendung unterstützt die Verwendung von Plugins. Plugins sind Softwareelemente, mit denen die Funktionen und Fähigkeiten der Anwendung verbessert werden und die das Benutzererlebnis optimieren. Möglicherweise gibt es für jeden Hub individuelle Plugins.
Die folgenden Plugins stehen zur Zeit für die Intel Unite Anwendung zur Verfügung:

Plugin für Gastzugang: Dieses Plugin ermöglicht es einem Computer, sich mit einem Hub zu verbinden, ohne dass er sich auf dem gleichen Unternehmensnetzwerk befinden muss und ohne die PIN-Validierung des Enterprise-Servers. Der Hub erstellt ein Ad-hoc-/gehostetes Netzwerk (Zugriffspunkt), zu dem ein Intel Unite Client eine Verbindung herstellen kann.

Plugin für Skype for Business: Dieses Plugin ist eine Lösung, um Personen aus einem Online-Skype-Meeting in eine Intel Unite App Sitzung mit einzubeziehen. Das Plugin läuft auf dem Hub der Intel Unite Software und verwaltet ein Mail-Konto speziell für jede Instanz.

Plugin für Telemetrie: Dieses Plugin fügt die Funktion hinzu, dass der Enterprise-Server Hub-Daten annimmt und anzeigt, wenn das Plugin auf dem Hub installiert ist. Mindestanforderung ist Enterprise-Server v3.0 (Build 3.0.38.44).

Darüber hinaus gibt es ein SDK zum Schreiben von Plugins:

Software-Development-Kit (SDK): Anleitung für die Anwendungsschnittstelle als Unterstützung für Software-Entwickler oder alle, die zusätzliche Funktionalität für die Intel Unite Anwendung entwickeln wollen.

Hinweis: Bitte beachten Sie die spezifischen Plugin-Anleitungen, wenn Sie einzelne Plugin-Komponenten installieren oder mehr über sie erfahren möchten.

5.6.1 Plugin-Installationshinweise

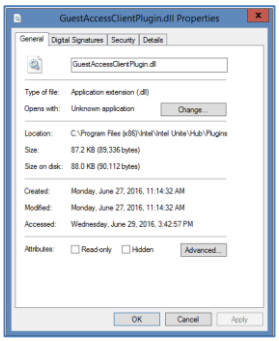
Jedes Plugin wird standardmäßig im Verzeichnis „Plugin“ im Installationsverzeichnis [Program Files(x86) \Intel\Intel Unite\Hub\Plugins\PluginName (Plugin.dll)] installiert. Plugins werden beim Start der Anwendung gezählt. Wenn ein neues Plugin hinzugefügt wird, muss die Anwendung neu gestartet werden. Bevor Sie das Plugin installieren, überprüfen Sie die Kompatibilität mit der Zielversion Ihrer Intel Unite Lösung. [beachten Sie die jeweilige Plugin-Anleitung, die Anforderungen variieren für die verschiedenen Plugins].
Stellen Sie auch sicher, dass Sie für jedes verwendete Plugin den Wert des Plugin-Zertifikats-Hash im Admin-Webportal erhalten und hinzufügen.
HINWEIS: Für eine Testumgebung können Sie auch den standardmäßigen Schlüsselwert verwenden, bei einer Produktionsumgebung wird jedoch davon abgeraten.

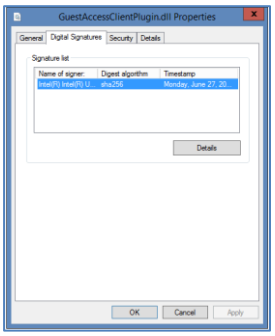
5.6.2 Wert für das Plugin-Zertifikats-Hash

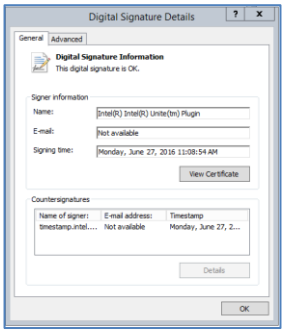
Befolgen Sie die nachstehenden Schritte, um den Wert des Zertifikats-Hashschlüssels für Ihr Plugin zu ermitteln:

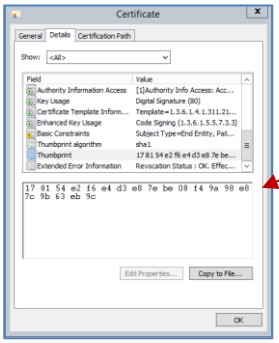
- Suchen Sie das Plugin im Plugin-Ordner, rechtsklicken Sie auf ***Plugin.dll** und wählen Sie **Eigenschaften** (z. B. GuestAccessClientPlugin.dll)
- Wenn sich das Plugin-Fenster **Eigenschaften** öffnet, suchen Sie und öffnen Sie die Registerkarte **Digitale Signaturen**.
- Wählen Sie hier **Intel Unite Plugin** aus und klicken Sie auf **Details**.
- Klicken Sie im Fenster **Details der digitalen Signatur** auf **Zertifikat anzeigen.**
- Im Fenster **Zertifikat** gehen Sie auf die Registerkarte **Details** und blättern nach unten, bis die Option **Fingerabdruck** erscheint.
- Wählen Sie **Fingerabdruck** und fügen Sie den Wert in eine Notepad- oder Text-Datei ein, sobald dieser angezeigt wird. Löschen Sie alle Leerzeichen und speichern Sie dann die Datei.

- Dieser Schlüsselwert wird verwendet, wenn Sie das Profil für Ihr Plugin erstellen. Dieser Schlüsselwert kann erstellt und eingegeben werden, nachdem das Profil erstellt wurde. Weitere Informationen hierzu finden Sie im folgenden Abschnitt.





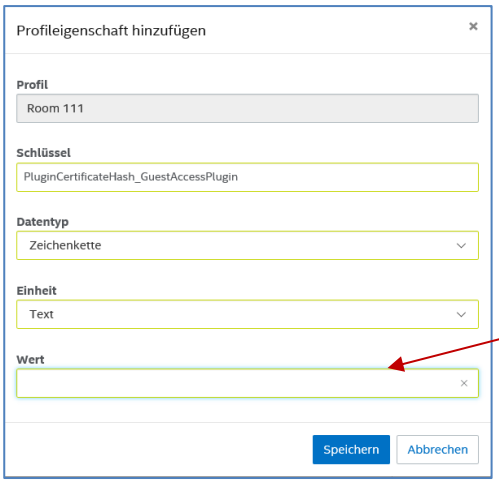




Kopieren Sie den Wert und fügen Sie ihn in ein Notepad-Fenster oder eine Textdatei ein. Dann entfernen Sie die Leerzeichen und speichern ihn ab.

5.6.3 Hinzufügen des Zertifikat-Hashs zu einem Plugin auf dem Admin-Webportal

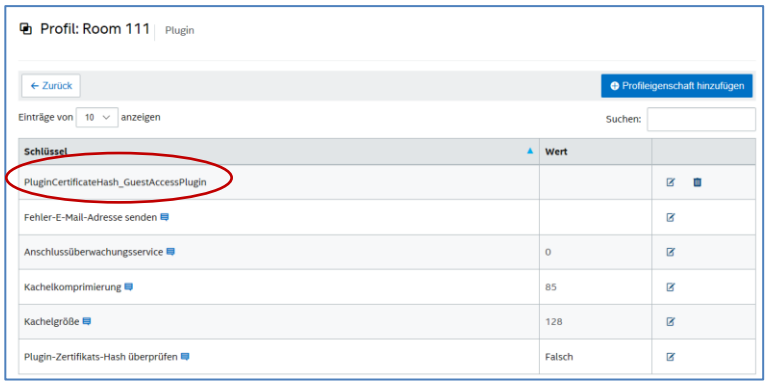
Wählen Sie unter **Gruppen** im Admin-Webportal das Profil aus, für das Sie das Plugin aktivieren möchten. Klicken Sie im Fenster „Profil“ auf **Profileigenschaft hinzufügen** und geben Sie Folgendes ein:



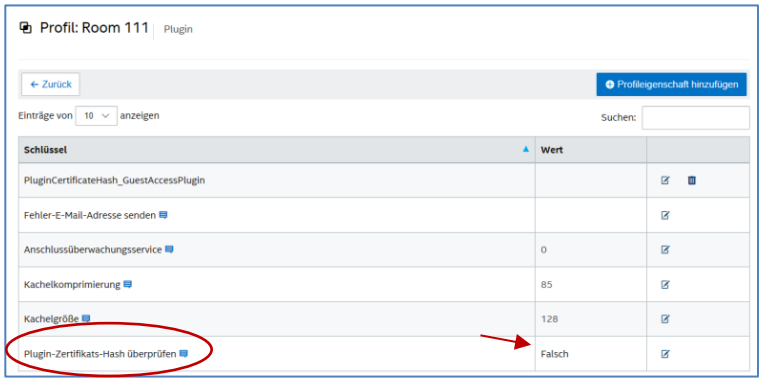
Verwenden Sie den Wert, der auf dem Notepad gespeichert ist, oder die Textdatei, die im vorigen Abschnitt beschrieben wurde. Stellen Sie sicher, dass der Wert korrekt ist (keine Leerzeichen).

- **Schlüssel**: PluginCertificateHash_XXX
    - XXX ist der Name des Plugins, für das der Hash hinzugefügt wird, z. B. GuestAccessPlugin. Zur einfacheren Identifizierung wird empfohlen, den Plugin-Namen zu verwenden, der dem Hash entspricht.
- **Datentyp**: Zeichenfolge
- **Einheit:** Text
- **Wert**: Fügen Sie den in der Notepad- oder Textdatei gespeicherten Fingerabdruckwert ein, siehe Abschnitt *Wert für das Plugin-Zertifikats-Hash*. Der Schlüsselwert kann auch nach der Schlüsselerstellung eingegeben werden.

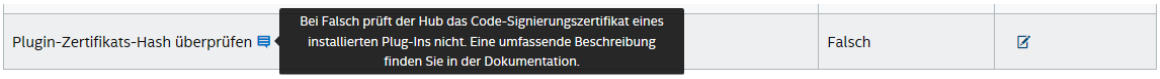
Klicken Sie auf **Speichern**. Sie können die Werte später über den Link **Bearbeiten** aktualisieren.
Der neue Schlüssel wird im Fenster „Profil“ angezeigt.



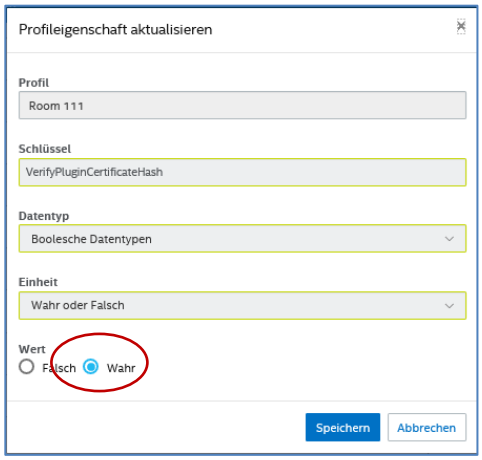
Sie müssen ebenfalls den Schlüssel **Plugin-Zertifikats-Hash überprüfen** aktivieren, indem Sie ihn auf „Wahr“ schalten; der Standardwert ist „Falsch“.



Sie können entscheiden, ob Sie das Plugin aktivieren oder deaktivieren wollen. Schalten Sie dazu den Schalter von „Wahr“ auf „Falsch“ oder umgekehrt. Denken sie daran, die Schlüsselwerte stellen die Gültigkeit des Plugin sicher.



Klicken Sie auf den Link **Bearbeiten**, um den Wert auf **Wahr** umzustellen und klicken Sie auf **Speichern**.



Die Plugin-Einstellungen wurden jetzt aktiviert.

6 Clientinstallation

6.1 Vor der Clientinstallation

Der Client muss den Enterprise-Server lokalisieren und bei ihm einchecken können. Die Intel Unite Anwendung benötigt eine Ausnahme in der Client-Firewall, um sich beim Enterprise-Server anmelden und mit ihm kommunizieren zu können.
Wenn Sie das Client-Installationsprogramm ausführen, werden Sie zur Eingabe der Server-Verbindungsdaten aufgefordert. Außerdem haben Sie die Möglichkeit, die manuelle Suche (die Option Server festlegen im Installationsprozess) zu umgehen und stattdessen die Informationen aus dem DNS-Diensteintrag zu übernehmen. Wenn Sie das Installationsprogramm ausführen, wird die Datei „ServerConfig.xml“ bearbeitet.

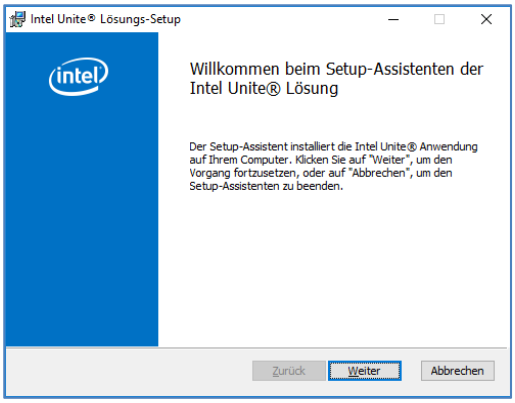
Je nach gewählter Methode für PIN-Lookup, müssen Sie wissen, ob **Automatische Suche nach Server** oder **Server angeben** während der Installation ausgewählt wurde.
Wenn Sie wissen, dass der DNS-Diensteintrag existiert, können Sie **Automatische Suche nach Server** auswählen. Es ist vorteilhaft, die automatische Suche zu verwenden, um Fehler bei der Eingabe zu vermeiden. Wenn Sie nicht sicher sind, wählen Sie die Option **Server angeben** (manuelle Suche), dafür müssen Sie jedoch den Hostnamen für den Enterprise-Server kennen.

Hinweis: Wenn in der Datei „ServerConfig.xml“ ein Server angegeben wurde, hat dieser Vorrang vor dem DNS-Diensteintrag.

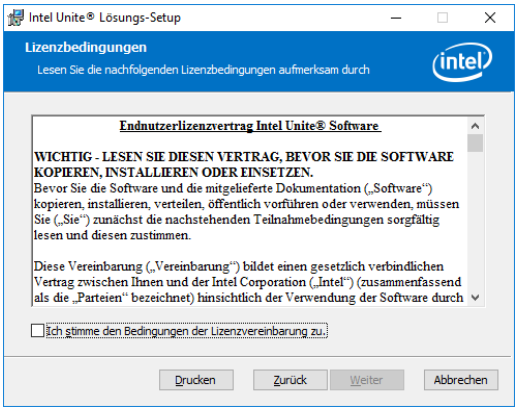
Mobile Client-Geräte: alle Client-Geräte müssen mit dem Unternehmensnetzwerk verbunden sein oder ein entsprechend konfiguriertes VPN verwenden. Die betrifft sowohl iOS- als auch Android-Geräte. Bei dem Versuch eine Verbindung mit der Intel® Unite™ App über ein normalerweise privat genutztes Tablet oder Mobiltelefon herzustellen, können Probleme auftreten, wenn das Tablet oder Mobiltelefon nicht über das Unternehmensnetzwerk, sondern über einen eigenen Mobilfunkanbieter verbunden ist, da die Firewall des Unternehmens diese Verbindung möglicherweise nicht zulässt. Für weitere Informationen siehe Abschnitt Mobile Client-Geräte.

6.2 Clientinstallation unter Windows

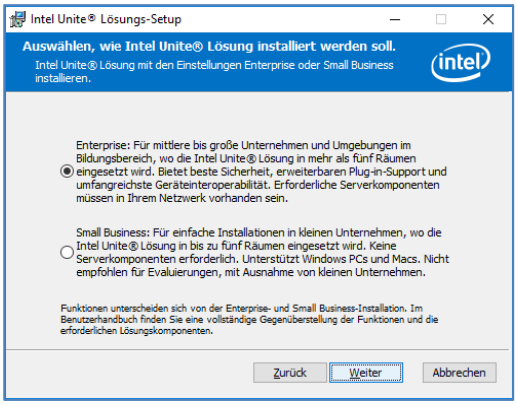
- Suchen Sie nach dem Installationsprogrammordner und führen Sie das Client-Installationsprogramm durch: **Intel Unite Client.mui.msi.** Klicken Sie auf **Weiter**, um fortzufahren.



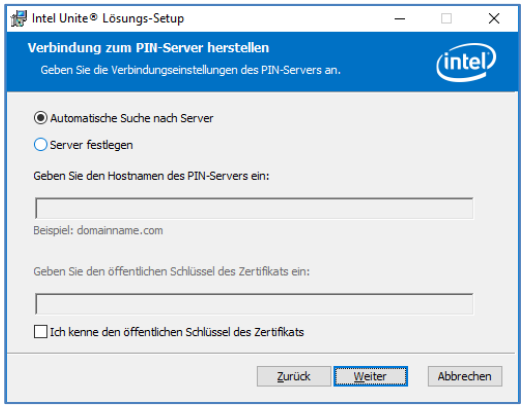
- Markieren Sie das Kontrollkästchen **Ich stimme den Bedingungen der Lizenzvereinbarung zu** und klicken Sie dann auf Weiter.



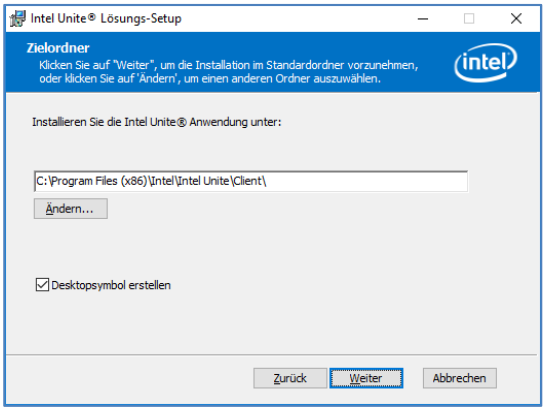
- Wählen Sie **Enterprise** aus und klicken Sie auf **Weiter**.



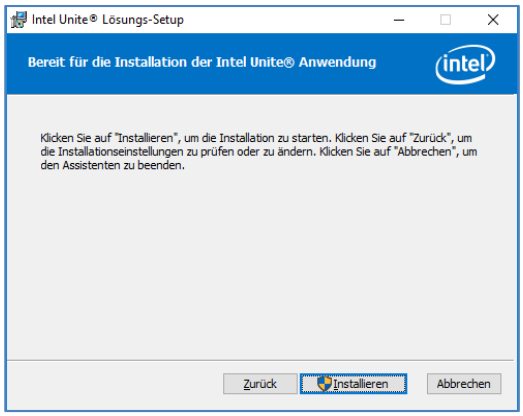
- In diesem Fenster müssen Sie die Verbindungseinstellungen für den PIN-Server angeben. Sie haben folgende Optionen zur Auswahl:
  - **Automatische Suche nach Server**: Dies ist die für Sie günstigste Wahl (Standard).
  - **Server festlegen**: In diesem Schritt muss Ihnen der Hostname des Enterprise-Servers bekannt sein
    - **Geben Sie den öffentlichen Schlüssel des Zertifikats ein**: diese Option wird aktiviert, wenn Sie **Server festlegen** auswählen.
    - Geben Sie den **öffentlichen Schlüssel des Zertifikats** ein, wenn er Ihnen vorliegt und Sie diese Methode gewählt haben.
- Treffen Sie Ihre Auswahl und klicken Sie dann auf **Weiter**.



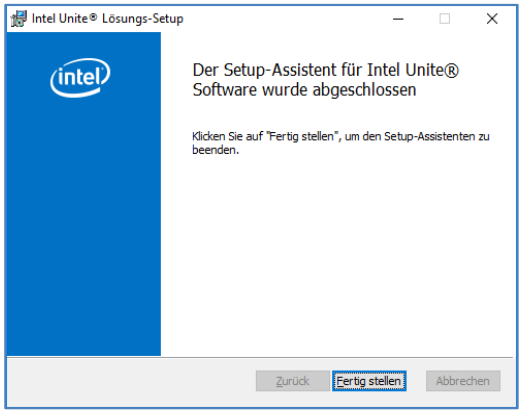
- Das Fenster **Zielordner** wird mit dem Standardordner geöffnet, in dem die Intel Unite Anwendung auf dem Client installiert wird; Sie können den Zielordner, falls gewünscht, ändern oder den Standardspeicherort beibehalten.



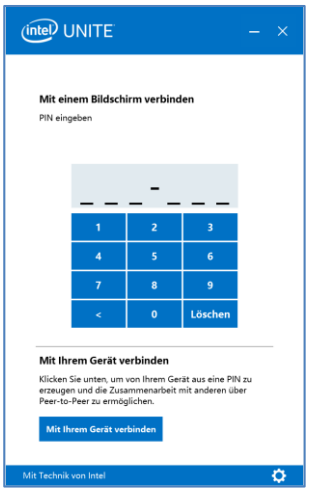
- Sie können zurückgehen, um Ihre Einstellungen zu überprüfen oder Sie können auf **Installieren** klicken, um den Vorgang fortzusetzen.



- Nach Abschluss der Installation wird Ihnen das Fenster **Der Setup-Assistent für Intel Unite® Software wurde abgeschlossen** angezeigt. Klicken Sie auf **Fertig stellen**.



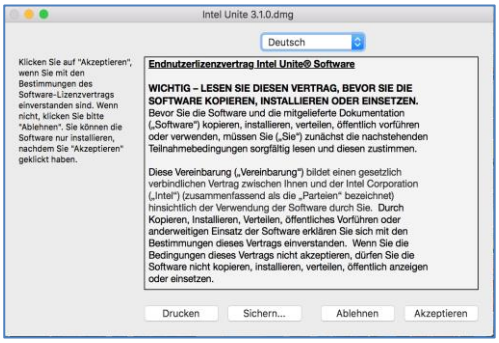
- Das folgende Fenster **Mit einem Bildschirm verbinden** wird angezeigt:



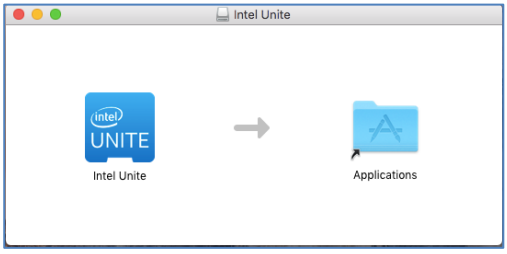
- Geben Sie zum Anschluss an den Hub die PIN-Nummer ein, die auf dem Bildschirm oder der Anzeige gezeigt wird. Standardmäßig ändert sich der PIN alle fünf Minuten.
- Im **Benutzerhandbuch der Intel Unite® Lösung** finden Sie Informationen zu Funktionen und Benutzerinformationen.

6.3 macOS Client-Installation

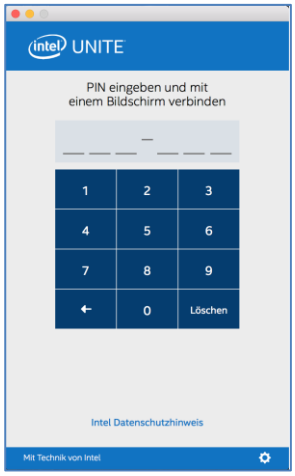
- Suchen Sie die Datei Intel Unite macOS X,X.dmg und laden Sie die Software auf Ihren Mac-Client herunter. Doppelklicken Sie auf die Datei, um die Anwendung zu entpacken.
- Sie werden dazu aufgefordert, dem Endbenutzer-Lizenzvertrag zuzustimmen. Klicken Sie auf Akzeptieren.



- Wenn sie extrahiert ist, bewegen Sie die Anwendung per Drag-and-Drop in den Ordner „Anwendungen".

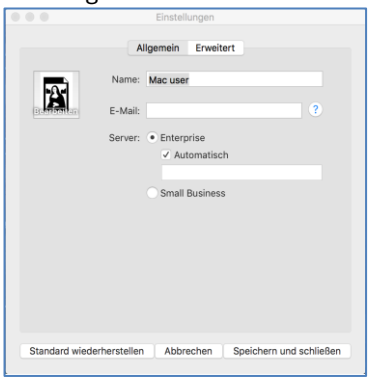


- Suchen Sie die Anwendung im Ordner „Anwendungen" und klicken Sie darauf, um sie zu starten.
- Der Bildschirm **PIN eingeben und mit einem Bildschirm verbinden** wird geöffnet. Sie können eine Verbindung zum Hub herstellen, indem Sie die PIN eingeben, der auf dem Bildschirm oder der Anzeige angezeigt wird, und die Freigabe starten.



- Im **Benutzerhandbuch der Intel Unite® Lösung** finden Sie Informationen zu Funktionen und Benutzerinformationen.

Hinweis: Die Anwendung verwendet DNS Auto Discovery (DNS-Diensteintrag), um den Enterprise-Server zu suchen. Sie können auch einen standardmäßigen Enterprise-Server festlegen und dazu die Einstellungen für com.intel.Intel-Unite.plist ändern, die sich im Ordner ~/Library/Preferences des Benutzers befinden:
defaults write com.intel.Intel-Unite EnterpriseServer myServer.mydomain.myTLD . Weitere Informationen finden Sie im Abschnitt *Intel Unite-Lösung für macOS* dieses Handbuchs.
Sie können auch den Enterprise-Server ändern, zu dem die Anwendung eine Verbindung herstellt. Klicken Sie auf das Zahnradsymbol in der unteren rechten Ecke des **Verbindungsbildschirms**, um auf die **Einstellungen** zuzugreifen.
Zwei Registerkarten stehen zur Verfügung:

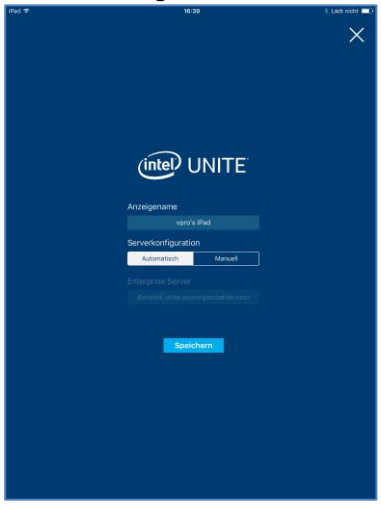


Allgemein: Sie können den Namen, die E-Mail-Adresse und den Avatar des Benutzers eingeben. Sie können auch entscheiden, ob sich das Client-Gerät automatisch mit dem Enterprise-Server verbindet (Standardeinstellung) oder durch Eingabe eines festgelegten Pfads.
Erweitert: Über diese Registerkarte können Sie den **Debugmodus aktivieren** oder einstellen, dass **nur vertrauenswürdige Zertifikate zugelassen** werden.

6.4 iOS Client-Installation

Die App ist kompatibel mit allen iPads mit Ausnahme des Original iPads von 2010.

- Gehen Sie auf Ihrem iOS-Client (d. h. Ihrem iPad-Gerät) zum Apple App Store und laden Sie die Intel Unite Software für Ihren Client herunter.
- Sobald die App heruntergeladen wurde, öffnen Sie die App.
- Klicken Sie auf das Zahnradsymbol in der oberen rechten Ecke, um auf die **Einstellungen** zuzugreifen und die erforderlichen Informationen einzugeben.



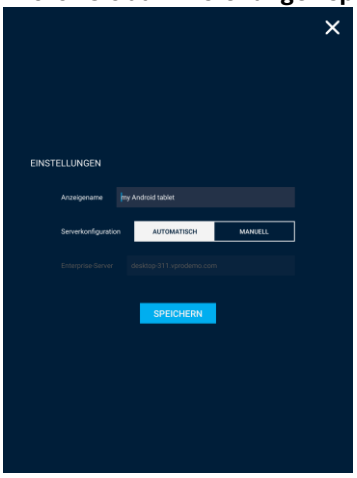
- Geben Sie unter **Einstellungen** Ihren gewählten Anzeigenamen und Ihre Serverinformationen ein.

- Sie können **Automatisch** auswählen, um den Server zu suchen oder wenn die Verbindung zu einem bestimmten Server hergestellt werden soll, klicken Sie auf **Manuell** und geben den Server für die Verbindung ein.
- Klicken Sie auf **Speichern**.
- Sie können eine Verbindung zum Hub herstellen, indem Sie die PIN eingeben, die auf dem Bildschirm oder der Anzeige angezeigt wird, und die Freigabe starten.
- Im **Benutzerhandbuch der Intel Unite® Lösung** finden Sie Informationen zu Funktionen und Benutzerinformationen.

6.5 Android Client-Installation

- Gehen Sie auf Ihrem Android-Gerät zum Google App Store und laden Sie die Intel Unite-Software für Ihren Client herunter.
- Sobald die App heruntergeladen wurde, öffnen Sie die App.
- Klicken Sie auf das Zahnradsymbol in der oberen rechten Ecke, um auf die **Einstellungen** zuzugreifen und die erforderlichen Informationen einzugeben.

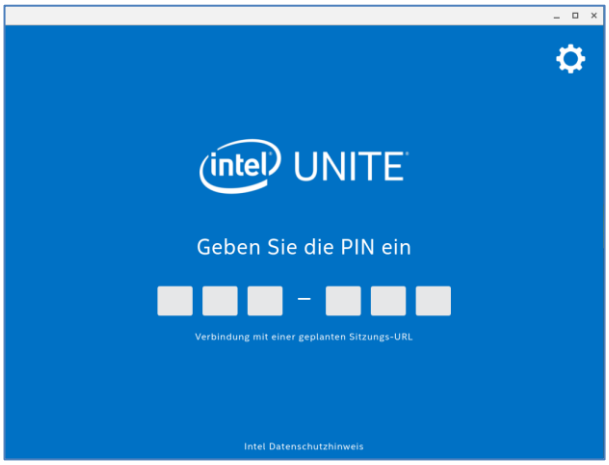
- Geben Sie unter **Einstellungen** Ihre gewählten Bildschirmnamen und Serverinformationen ein.
- Sie können **Automatisch** auswählen, um den Server zu suchen oder wenn die Verbindung zu einem bestimmten Server hergestellt werden soll, klicken Sie auf **Manuell** und geben den Server für die Verbindung ein.
- Klicken Sie auf **Einstellungen speichern.**



- Sie können eine Verbindung zum Hub herstellen, indem Sie die PIN eingeben, die auf dem Bildschirm oder der Anzeige angezeigt wird, und die Freigabe starten.
- Im **Benutzerhandbuch der Intel Unite® Lösung** finden Sie Informationen zu Funktionen und Benutzerinformationen.

6.6 Chrome OS Client-Installation

- Gehen Sie auf Ihrem Chromebook-Gerät zum Apple App Store und laden Sie die Intel Unite Software für Ihren Client herunter.
- Sobald die App heruntergeladen wurde, öffnen Sie die App.
- Klicken Sie auf das Zahnradsymbol in der oberen rechten Ecke, um auf die **Einstellungen** zuzugreifen und die erforderlichen Informationen einzugeben.



- Geben Sie unter Einstellungen Ihren gewählten Bildschirmnamen, Ihre E-Mail-Adresse und Serverinformationen ein. Sie können **Automatisch** auswählen, um den Server zu suchen oder wenn die Verbindung zu einem bestimmten Server hergestellt werden soll, klicken Sie auf **Manuell** und geben den Server für die Verbindung ein.
- Klicken Sie auf **Einstellungen speichern.**

Sie können eine Verbindung zum Hub herstellen, indem Sie die PIN eingeben, die auf dem Bildschirm oder der Anzeige angezeigt wird, und die Freigabe starten.
Im Benutzerhandbuch der Intel Unite® Lösung finden Sie Informationen zu Funktionen und Benutzerinformationen.

6.7 Client-Konfiguration

Client-Konfigurationseinstellungen können über das Admin-Portal geändert werden. Im Admin-Portal ist ein Standardprofil mit Standardkonfigurationseinstellungen enthalten, das auf alle Clients angewendet wird, die beim Server einchecken. Die Konfigurationsoptionen werden an den Client weitergegeben, nachdem eine Verbindung vom Client mit dem Enterprise-Server hergestellt wurde. Die Einstellungen werden bei jedem Einchecken des Clients aktualisiert.
Für weitere Informationen zu Ihren Konfigurationsoptionen siehe Profilkonfiguration .

7 Erweiterte Installation

7.1 Skript-Installationsprogramme

Dieser Abschnitt bietet Informationen über das Ausführen der Installationsprogramme im stillen (unbeaufsichtigten) Modus, ohne dass Menüs oder Fenster erscheinen. Auf diese Weise werden Property-Parameter über die Befehlszeile an das Installationsprogramm übergeben.
Öffnen Sie die Befehlsaufforderung, um die unbeaufsichtigten Installationsprogramme auszuführen und verwenden Sie die folgende Befehlszeile:
msiexec /i "PFAD_ZU_CLIENT_MSI" PARAMETER=VALUE PARAMETER=VALUE ... /qn /l* "PFAD_ZU_PROTOKOLL"

- Das /i kennzeichnet das angegebene MSI für die Installation. „PATH_TO_CLIENT_MSI“ ist der Dateiname des Installationsprogramms, das Sie aufrufen.
- „PARAMETER=VALUE PARAMETER=VALUE ...“ ist eine Liste mit den in der Tabelle unten angegebenen Parametern.
- Das Attribut /qn führt das Installationsprogramm im stillen Modus aus.
- Das Attribut /l* protokolliert Ausgabe an die Protokolldatei, die Sie angeben.

HINWEIS: Sie können alle Optionen für **msiexec** sehen, indem Sie den folgenden Befehl ausführen:
msiexec /?
Im Folgenden finden Sie die vollständige Liste der Property-Parameter, die an den jeweiligen Installer übergeben werden können:

Serverinstallationsparameter	Beschreibung
DBHOSTNAME = “local” oder “{IP}” oder “{server},{port}” (die Standradeinstellung ist „local“)	Hostname des Microsoft SQL Server. Hier erstellt das Installationsprogramm die UniteServer-Datenbank und fügt das Datenbank-Dienstkonto hinzu. Wenn die Datenbank auf dem aktuellen Computer installiert wird, müssen Sie diesen Parameter nicht angeben, da „lokal“ bereits der Standardwert ist.
DBLOGONTYPE = “WinAccount” oder “SqlAccount” → Standardwerte zu WinAccount	Legt den Anmeldungstyp für den Zugriff auf den Microsoft SQL Server fest. Optionen sind Windows-Authentifizierung oder SQL-Authentifizierung.
DBUSER = “{SQL username}” DBPASSWORD = “{SQL password}”	Wenn der Anmeldungstyp SqlAccount ist, geben Sie den Benutzernamen und das Passwort ein. HINWEIS: Dieses Konto muss über Berechtigungen zum Hinzufügen der Datenbank und zum Erstellen des Datenbank-Dienstkontos verfügen.
DBLOGONPASSWORD = “{service account password}”	Das vom Dienstkonto zum Herstellen der Verbindung mit der UniteServer-Datenbank zu verwendende Passwort.
DBLOGONPASSWORDCONF = “{service account password}”	Diese Variable muss den gleichen Wert haben, der in DBLOGONPASSWORD angegeben ist
Serverfunktions-Auswahlparameter	**Beschreibung**

ADDLOCAL = “ALL”	Es gibt nur zwei Optionen: ALL = Installieren von Datenbank UND PIN-Server, Admin-Portal und Downloadseite. (diese Variable nicht angeben) = Installieren von PIN-Server, Admin-Portal und Downloadseite.
Client- und Hub-Installationsparameter	**Beschreibung**
PINSERVERLOOKUPTYPE = “Lookup” oder “Manual” die Standradeinstellung ist „Lookup“	Legt fest, wie die Anwendung den PIN-Server findet. „Lookup“ verwendet den DNS-Diensteintrag, während bei „Manual“ die Eingabe der Parameter PINSERVER erforderlich ist.
PINSERVER = “{hostname}”	Der Hostname des Servers, zu dem die Verbindung hergestellt werden soll.
CERTKEYCHECKED = “1” oder “0” Die Standradeinstellung ist „0“	Dieser Parameter ist optional 0 = Schlüsselhash des Zertifikats nicht überprüfen 1= Schlüsselhash des Zertifikats überprüfen, CERTKEY muss auch angegeben werden.
CERTKEY = “{certificate key}”	Dieser Parameter ist optional Geben Sie den öffentlichen Schlüssel des Zertifikats des PIN-Servers ein.
VERKNÜPFUNGEN	optional Auf „1“ setzen, um Desktop-Verknüpfungssymbole zu platzieren.
INSTALLTYPE = zwei mögliche Werte „Enterprise“ und „StandAlone“.	Wenn der INSTALLTYPE „Enterprise“ ist, dann wird der Client/Hub als Enterprise installiert. Wenn der INSTALLTYPE „StandAlone“ ist, dann wird der Client/Hub als Standalone installiert.
SKIP_EXTENDED_DISPLAY= „1“ oder „0“ Die Standradeinstellung ist „0“	0 = Falsch 1 = Richtig

7.2 Registrierungsschlüssel

Die Registrierungsschlüssel werden in die Registrierungsdatenbank geschrieben, wenn Sie die Installationsprogramme und die Anwendung ausführen. Werte in einigen dieser Schlüssel können gemäß des gewünschten Ergebnisses angepasst werden. In der Liste unten werden die Schlüssel erklärt, die von der Intel Unite Anwendung geschrieben werden:

Registrierungsschlüssel: (aktueller Benutzer)	Wert	Gerät
HKEY_CURRENT_USER\software\Intel\Unite\ ActiveConnection (DWORD)	[0 = keine verbundenen Benutzer 1 = verbundene Benutzer]	Hub

HKEY_CURRENT_USER\software\Intel\Unite\ PublicKey (String)	[öffentlicher Schlüssel des Verbindungs-zertifikats]	Beide
HKEY_CURRENT_USER\software\Intel\Unite\ CurrentPin (string)	[aktuelle PIN dieses Systems]	Hub
HKEY_CURRENT_USER\software\Intel\Unite\ DoNotShowPrivacyStatement (DWORD)	[0 = Datenschutzerklärung beim Start 1 = Datenschutzerklärung nicht anzeigen]	Beide
HKEY_CURRENT_USER\software\Intel\Unite\ HWThumbprint (String)	[Hash von HW]	Beide
HKEY_CURRENT_USER\software\Intel\Unite\ ServicePort (DWORD)	[Port, den dieser Service abhört]	Hub
HKEY_CURRENT_USER\software\Intel\Unite\ ActivePresenter	[1 = Client präsentiert 0 = kein Client präsentiert]	Hub
HKEY_CURRENT_USER\software\Intel\Unite\PinPadWindows (DWORD)	[1 = Anwendung ist für die PIN-Eingabe bereit 0 = andernfalls]	Client
HKEY_CURRENT_USER\software\Intel\Unite\GuestAccess\SSID Referenz: Plugin Benutzerhandbuch für GASTZUGANG	Durch Festlegen eines Standardwerts erhöht sich das Sicherheits-risiko beim Gastzugang	Hub
HKEY_CURRENT_USER\software\Intel\Unite\GuestAccess\PSK Referenz: Plugin Benutzerhandbuch für GASTZUGANG	Durch Festlegen eines Standardwerts erhöht sich das Sicherheits-risiko beim Gastzugang	Hub
HKEY_CURRENT_USER\software\Intel\Unite\GuestAccess\Download Referenz: Plugin Benutzerhandbuch für GASTZUGANG	Der Standard-Downloadlink lautet http://192.168.173.1/download	Hub
HKEY_CURRENT_USER\software\Intel\Unite\ShowAvToggle (DWORD) = 1 (A/V Modus Umschalter Aktivieren/Deaktivieren)	Win7 Aero-Modus. Ermöglicht es dem Benutzer, zwischen RTF und WebRTC umzuschalten.	Client
Registrierungsschlüssel: (Maschine):	**Wert**	**Gerät**
HKEY_LOCAL_MACHINE\software\Intel\Unite\ HubUnlockPassword (String)	[Passwort für das Beenden der Hub-Anwendung]	Hub
HKEY_LOCAL_MACHINE\software\Intel\Unite\ DisableCheckCertificateChain (DWORD)	[Für selbstsignierte Zertifikate festgelegt, der Wert 1 bedeutet, dass die Zertifikatkette von Enterprise (Serverzertifikat) nicht geprüft wird]	Beide

HKEY_LOCAL_MACHINE\software\Intel\Unite\ DisableUsageCollection (DWORD)	[1 = Telemetrie-Datensammlung deaktivieren]	Beide
HKEY_LOCAL_MACHINE\software\Intel\Unite\WindowedMode (DWORD) (funktioniert nur im Small-Business-Modus, nicht im Enterprise-Modus)	[1 = der Benutzer will den Hub im Fenstermodus starten (mit den Schaltflächen „minimieren“, „maximieren“ und „schließen“) 0 = andernfalls]	Hub
HKEY_LOCAL_MACHINE\software\Intel\Unite\AllowInsecureCertificates (DWORD)	[1 = Zertifikat-Algorithmusprüfung wird übersprungen 0 = das Enterprise-Zertifikat wird gezwungen, ein SHA2-Zertifikat zu verwenden]	Beide
HKEY_LOCAL_MACHINE\software\Intel\Unite\ShowOnlyInOneMonitor (DWORD)	[Dieser Schlüssel funktioniert nur, wenn der Fenstermodus auf 1 gesetzt ist. 1 = Es wird nur ein PIN-Fenster angezeigt, obwohl mehrere Bildschirme angeschlossen sind]	Hub
HKEY_LOCAL_MACHINE\SOFTWARE\Intel\Unite\S4BPlugin Keywords (String) = Komma,getrennte,Liste,von,Keywords	Schlüssel, der für das Plugin für Skype for Business verwendet wird	Hub
HKEY_LOCAL_MACHINE\software\Intel\Unite\ LogFile (String)	[Pfad zum Dateinamen mit Schreibzugriff auf Protokolllaufzeit-Debugmeldungen]	Beide

8 Leitfaden für das Admin-Portal

Das Admin-Portal ist das Administrator-Webportal für die Intel Unite Anwendung, in dem Sie die Geräte, auf denen die Intel Unite Anwendung installiert ist, anzeigen und verwalten können. Es ist eine der Komponenten, die während der Installation zusammen mit dem PIN-Dienst und dem Webserver auf dem Enterprise-Server installiert wird. (Siehe Abschnitt Installation des Enterprise-Servers). Das Admin-Portal muss sich nicht auf dem gleichen Server wie die Datenbank befinden, solange es Zugriff auf die Datenbank hat.

Zusätzlich zu den neuen Funktionen hat das Admin-Portal ein neues Aussehen erhalten; es wurden Hilfemenüs und Funktionsinformationen hinzugefügt, um die Konfiguration Ihres Hubs und der Client-Geräte zu vereinfachen.

- Wechseln Sie für den Zugriff auf das Admin-Portal zu Ihrem Browser und folgen Sie dem Link, der dem Portal zugewiesen ist. Dieser lautethttps://<yourservername>/admin, wobei <yourservername> der Name des Intel Unite Servers ist (Standard = UniteServer, d. h. https://uniteserver/admin)

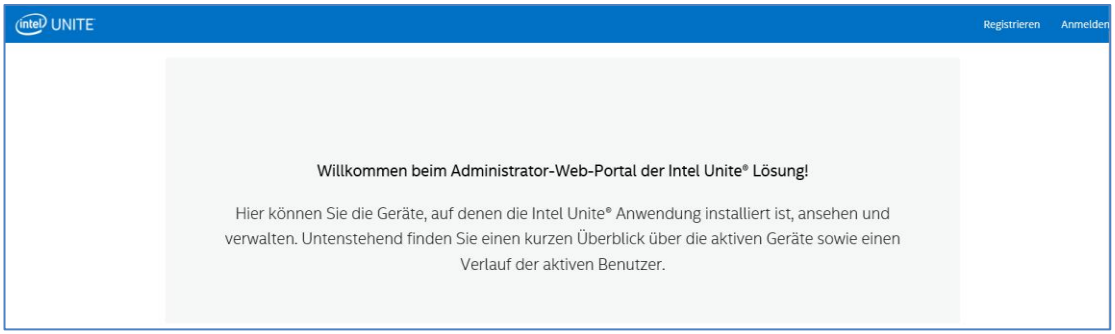
Als der IT-Administrator die Software-Installer ausführte, wurde ein Standard-Administratorkonto mit folgendem Benutzernamen und Passwort erstellt:

- Benutzer: admin@server.com
- Passwort: Admin@1

Dieses Konto hat vollständigen Zugriff auf das Admin-Portal und ermöglicht die Anmeldung; Sie werden jedoch aufgefordert, das Passwort zu ändern. Wenn Sie bereits ein Konto registriert haben, geben Sie Ihre Zugangsdaten ein, um Zugriff auf das Admin-Portal zu erhalten.

8.1 Willkommensseite des Admin-Webportals

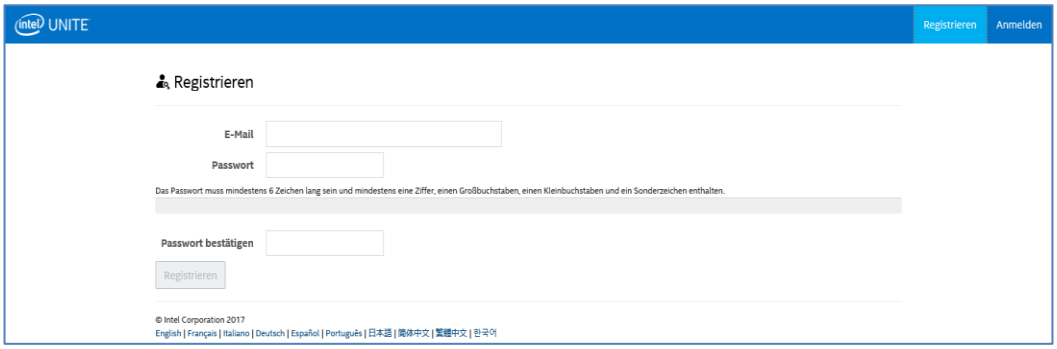
Die Willkommensseite wird angezeigt, sobald Sie sich mit dem Admin-Portal verbinden. Für den Zugriff auf die Homepage müssen Sie sich mit dem Standardkonto, das während der Installation erstellt wurde, oder mit Ihren Kontodaten anmelden.



8.1.1 Registrieren eines Kontos

Stellen Sie zum Registrieren eines Kontos sicher, dass Sie vom Admin-Portal abgemeldet sind.

- Klicken Sie auf **Registrieren** in der Navigationsleiste ganz oben rechts.
- Geben Sie in das Formular die entsprechende E-Mail-Adresse und ein Passwort ein und klicken Sie auf **Registrieren**.



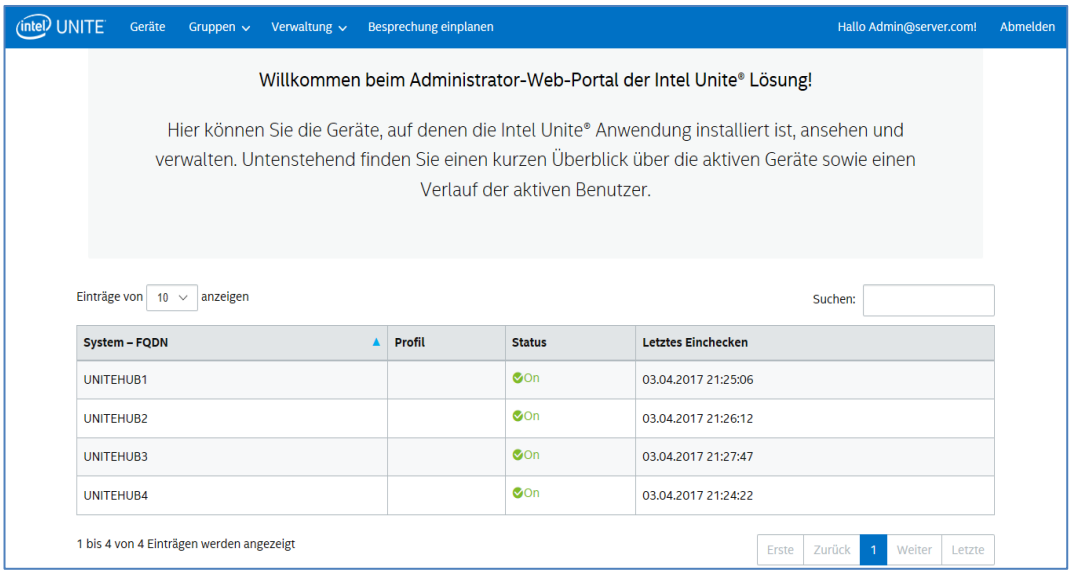
- Alternativ können Sie Benutzer über die Registerkarte „Verwaltung“ hinzufügen oder registrieren, nachdem Sie sich beim Admin-Portal angemeldet haben.

8.1.2 Anmeldung mit einem bestehenden Konto

Sie können sich mit einem registrierten Konto anmelden oder das während der Installation erstellte Standardkonto verwenden. Zur Erinnerung: Dieses Konto hat vollen Zugriff auf das Admin-Portal, wir empfehlen Ihnen, das Passwort zu ändern, um sicherzustellen, dass der Zugriff auf das Portal beschränkt ist.

8.2 Die Startseite des Admin-Portals

Die Startseite enthält eine Begrüßungsnachricht und bietet einen schnellen Überblick über alle aktiven Systeme – Clients und Hubs – die am Server angemeldet sind. Die Tabelle zeigt den Namen des jeweiligen **Systems**, das dem System zugeordnete **Profil**, den Ein- oder Aus-**Status** und Datum sowie Zeit des **letzten Eincheckens**.



Die Einträge der Tabelle können mithilfe des Suchfelds nach mehreren Schlüsselwörtern gefiltert werden. Alle Spalten werden nach jedem Schlüsselwort durchsucht. Sie können festlegen, wie viele Einträge in diesem Fenster angezeigt werden sollen, indem Sie auf „Zeige <Anzahl der> Einträge“ klicken. Sie können 10, 25, 50 oder bis zu 100 Einträge anzeigen.

8.2.1 Navigationsleiste

Die Navigationsleiste führt Sie zu den unterschiedlichen Bereichen des Webportals und zeigt außerdem den aktuell angemeldeten Benutzer oder die Schaltfläche **Registrieren** an, wenn kein Benutzer angemeldet ist.

Die Webportal-Seiten und Unterseiten sind:

- **Geräte**
- **Gruppen**
  - Gerätegruppe
  - Profile
- **Verwaltung**
  - Servereigenschaften
  - Benutzer
  - Rollen
  - Moderatoren
  - Reservierte PIN
  - Telemetrie
- **Besprechung einplanen**

Gehen Sie zum Abschnitt, der jedem Thema in diesem Kapitel des Admin-Portals zugeordnet ist, um mehr zu erfahren.

8.2.2 Nomenklatur der Symbole/Links

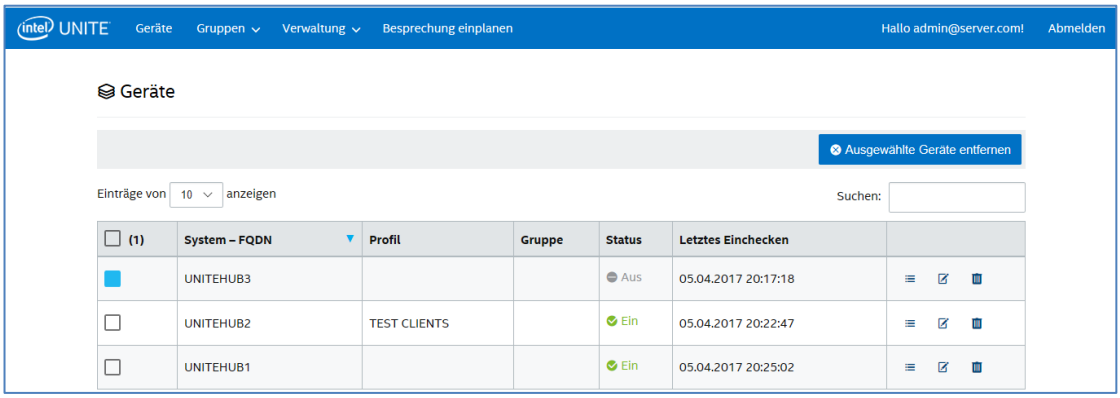
Im gesamten Web-Portal sehen Sie immer folgende Symbole oder Links:

	Bearbeiten
	Details anzeigen
	Geräte anzeigen
	Löschen
	Dialogfeld mit Informationen über einen bestimmten Wert

Platzieren Sie den Cursor über das Symbol, um Informationen zum jeweiligen Element anzuzeigen.

8.3 Geräte-Seite

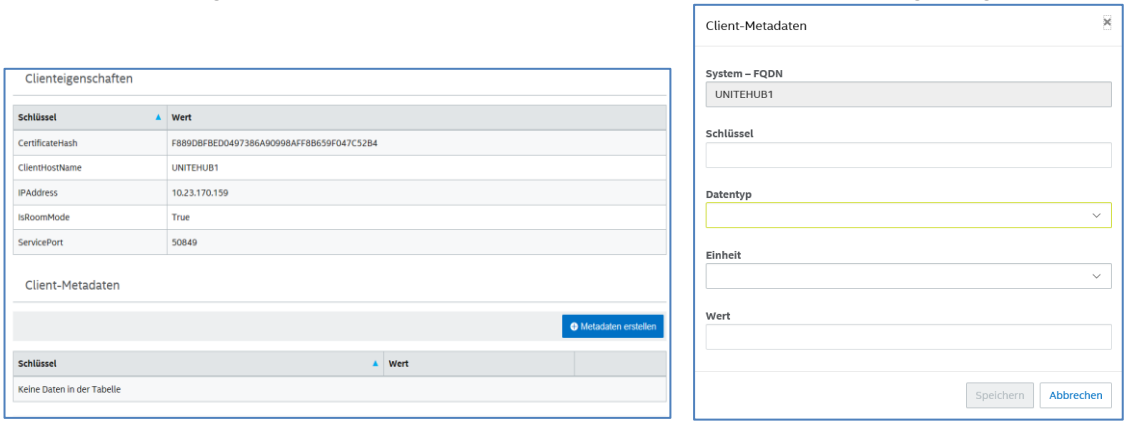
Auf der Geräte-Seite sehen Sie alle aktuell in der Datenbank vorhandenen Geräte. Sie können ein bestimmtes Gerät auswählen und dann entsprechend **Anzeigen**, **Bearbeiten**, **Aktualisieren** oder **Entfernen** wählen.



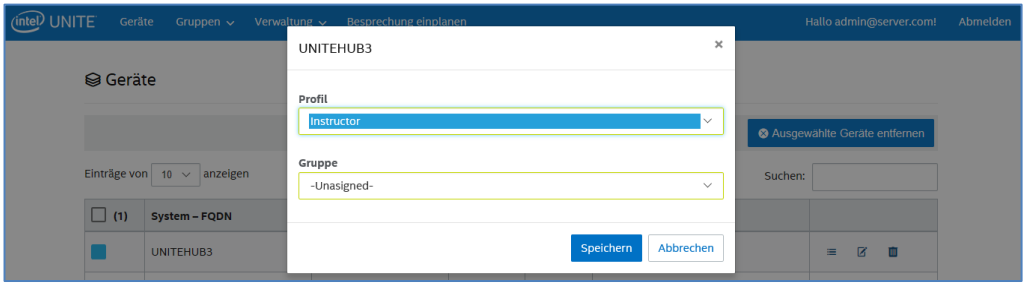
Auf der Seite **Geräte** finden Sie:

- **System-FQDN** ist der vollständig qualifizierte Domänenname des Clients/Hubs
- **Profil** verfügt über die Konfigurationseinstellungen, die für das Gerät angewandt werden
- **Gruppe** ist der Name der Gruppe, der ein Gerät zugewiesen wurde
- **Status** zeigt an, ob das Gerät aktiv EIN (grün) oder inaktiv AUS (grau) ist
- **Letztes Einchecken** ist der letzte Zeitpunkt, zu dem das Gerät beim Server angemeldet war
- **Details**: Wenn Sie auf den Link **Details anzeigen** klicken, wird das Fenster **Client-Eigenschaften** eingeblendet, das die Systemeigenschaften und Metadaten zeigt. Einige der Schlüssel unter **Client-Eigenschaften** sind:
    - CertificateHash
    - ClientHostName
    - IPAddress
    - IsRoomMode
    - SevicePort

Weitere Informationen über gültige Werte für jeden Schlüssel finden Sie im Abschnitt Profilkonfiguration zu detaillierten Informationen zu Schlüsseln und den zugehörigen Werten.



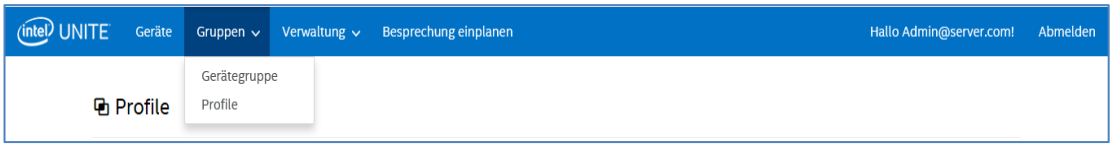
Link **Bearbeiten** – Klicken auf den Link „Bearbeiten“ ermöglicht das Bearbeiten des Geräteprofils und die Zuweisung des Geräts zu einer bestimmten Gruppe



Link **Löschen** – Klicken auf den Link „Löschen“ entfernt das Gerät vom Admin-Portal, Sie erhalten eine Bestätigungsmeldung, bevor das Gerät entfernt wird. Alternativ können Sie in der linken Spalte eines oder mehrere Geräte auswählen und auf die Schaltfläche **Ausgewählte Geräte entfernen** klicken.

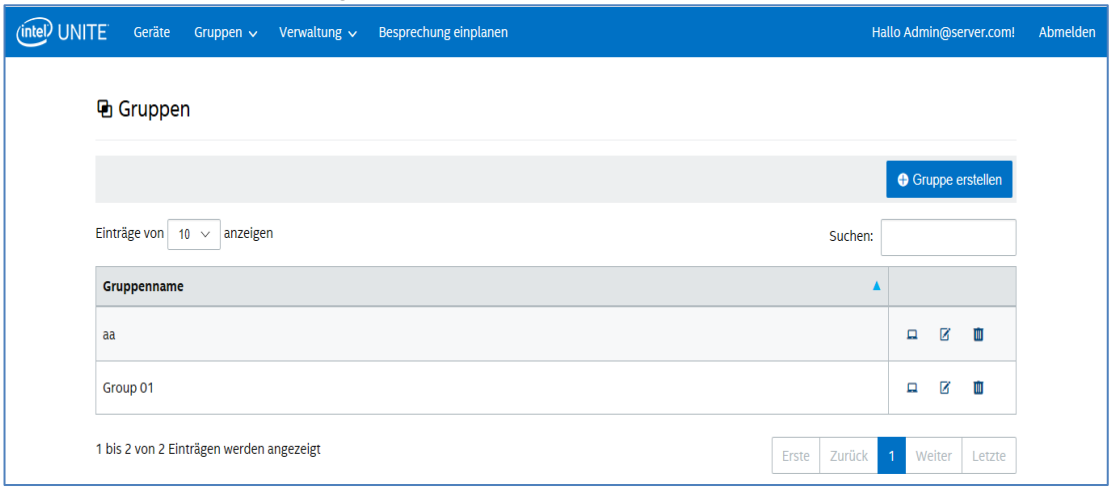
8.4 Gruppen-Seite

Auf der Seite **Gruppen** haben Sie im Menü zwei Optionen: **Gerätegruppe** und **Profile**.



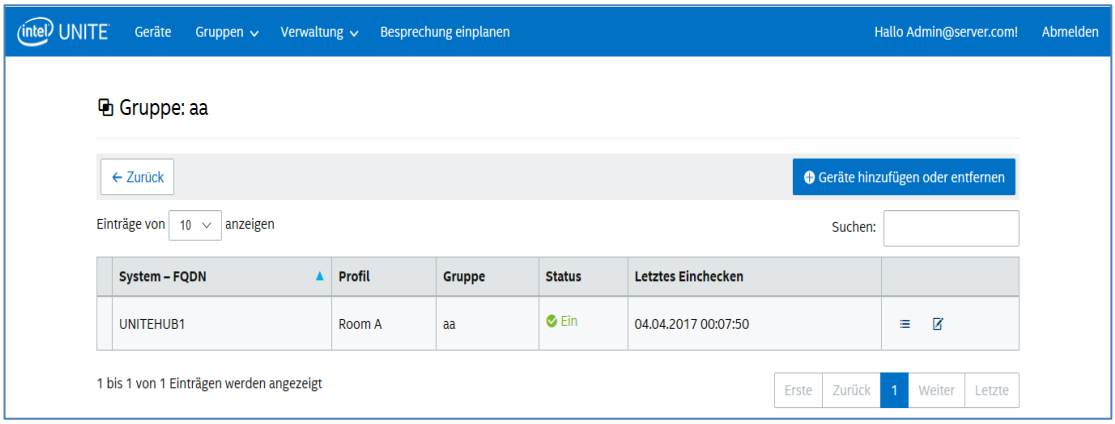
8.4.1 Gruppen > Gerätegruppe

Gerätegruppe bietet die Möglichkeit, Geräte zur Überwachung, für Funktionalität und Komfort zusammen zu gruppieren. Sie können Geräte mit demselben oder mit unterschiedlichen Profilen einer Gruppe zuordnen. Auf dieser Seite können Sie die Gruppen und Einträge für jede Gruppe erstellen, anzeigen, bearbeiten und löschen. Sie können eine neue Gruppe erstellen, indem Sie auf Gruppe erstellen klicken und den Namen der Gruppe angeben.



Sobald die Gruppe erstellt wurde, ist Folgendes verfügbar:

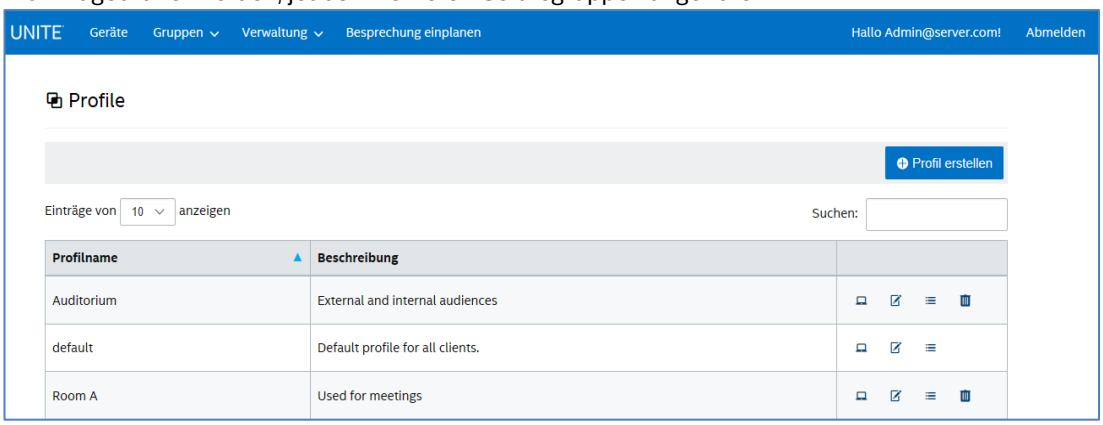
- Klicken Sie auf **Geräte anzeigen**, um Geräte zur ausgewählten Gruppe hinzuzufügen oder aus dieser zu entfernen. Alternativ können Sie auf den Link **Details** in der rechten Spalte klicken, um die Eigenschaften und die Metadaten jedes Systems anzuzeigen, das zu dieser Gruppe gehört.



- Klicken Sie auf den Link **Bearbeiten**, um den **Gruppennamen** zu aktualisieren oder zu ändern.
- Klicken Sie auf **Speichern**, um vorgenommene Änderungen beizubehalten.

8.4.2 Gruppen > Profile

Auf dieser Seite können Sie die Profile erstellen, anzeigen, löschen und bearbeiten. Diese Seite ist der Seite **Gerätegruppen** in Layout und Funktion ähnlich, enthält jedoch Profile. Der Unterschied zwischen **Profilen** und **Gruppen** ist, dass Profile die Konfigurationsoptionen für Geräte enthalten. Geräte können nur einem Profil zugeordnet werden, jedoch mehreren Gerätegruppen angehören.



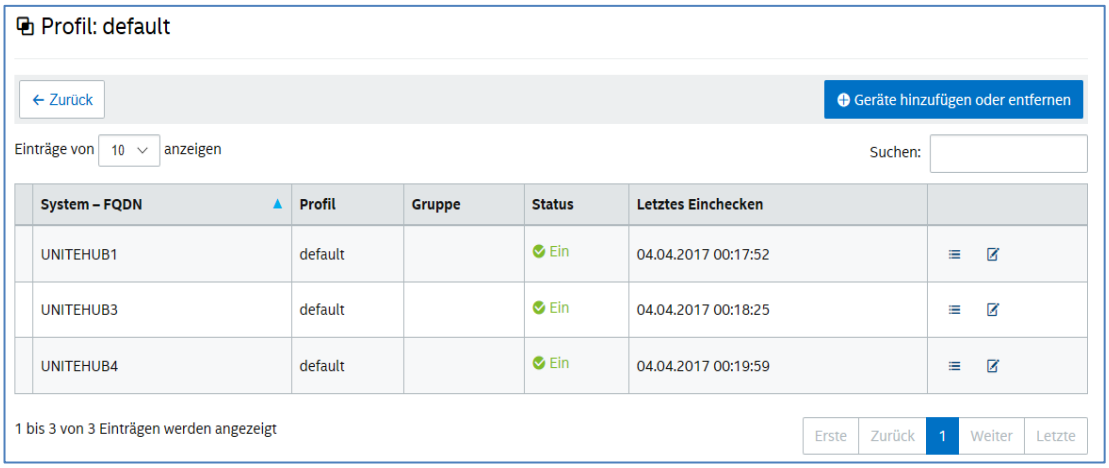
Die Seite **Profile** zeigt den **Profilnamen** und die **Beschreibung** jedes Profils, das auf dem Server verfügbar ist. Profile werden auf alle Geräte angewandt, die sich mit dem Enterprise-Server anmelden. Sie werden feststellen, dass das **StandardProfil** im Admin-Portal nicht gelöscht werden kann.

Nachdem Sie auf den Link **Geräte anzeigen** klicken, sehen Sie die Systeme, die dem ausgewählten Profil zugewiesen wurden.
Indem Sie auf den Link **Bearbeiten** klicken, können Sie den Namen des Profils und seine Beschreibung aktualisieren.

Nachdem Sie auf den Link **Details anzeigen** eines bestimmten Profils klicken, können Sie auf den Schlüssel und die Einstellungen der Werte des Standardprofils oder des neu erstellten Profils zugreifen und diese bearbeiten. Es wird eine Liste mit allen Schlüsseln, ihren Werten und dem Link **Bearbeiten** für die Aktualisierung oder entsprechende Anpassung angezeigt. Siehe Abschnitt *Profilkonfiguration* für detaillierte Informationen zu Schlüsseln und den zugehörigen Werten.

8.4.2.1 Standardprofil

Das **Standardprofil** kann nicht im Admin-Portal gelöscht werden. In dem Wissen, dass das Standardprofil nicht gelöscht wird, können Sie andere Profile erstellen.

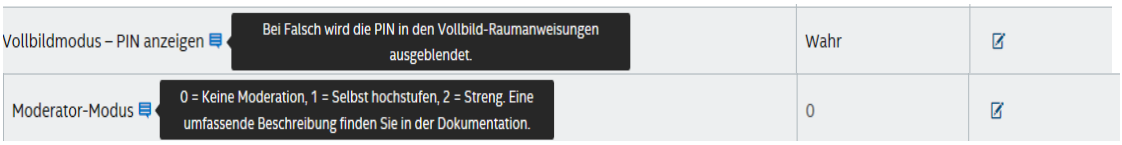


Standardschlüssel und -werte:

Schlüssel	Wert
Datei-Übertragung erlauben	Falsch
Support für Audio-/Video-Streaming	Wahr
PIN während Besprechung ändern	Wahr
Remote-Ansicht deaktivieren	Falsch
Größe der PIN anzeigen	48
Transparenz für PIN-Anzeige	100
Erweiterungen blockierter Dateien	
Max. Dateigröße	2147483647
Vollbildmodus	Wahr
Hintergrundfarbe Vollbildmodus	
Vollbildmodus – Hintergrundbildstreckung	Falsch
Vollbildmodus - Hintergrundfarbe-URL	
Vollbildmodus - Anweisungen	{pin}
Vollbildmodus – PIN-Farbe	
Vollbildmodus – PIN anzeigen	Wahr
Vollbildmodus - Schriftfarbe	
Vollbildmodus - Schriftart	
Hub - Tastatur sperren	Falsch
Hub - Uhr anzeigen	Wahr
Moderator-Modus	0

Fehler-E-Mail-Adresse senden		
Anschlussüberwachungsservice	0	
Kachelkomprimierung	85	
Kachelgröße	128	
Plugin-Zertifikats-Hash überprüfen	Wahr	

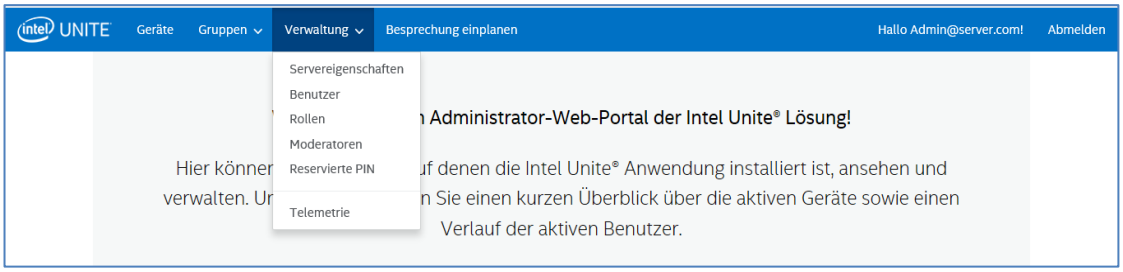
Bitte beachten Sie, dass neben jedem Schlüssel ein Dialogfeld zu finden ist. Indem Sie den Cursor auf das Dialogfeld platzieren, sollten Sie die Werte und/oder Informationen über jeden Schlüssel sehen können. Dadurch erhalten Sie die Informationen, die Sie vor dem Bearbeiten des Schlüssels benötigen. Siehe die beiden Beispiele unten:



Detaillierte Schlüssel und die dazugehörigen Werte siehe auch Tabelle unter Profilkonfiguration.

8.5 Verwaltungsseite

Die Verwaltungsseite hat mehrere Unterseiten:

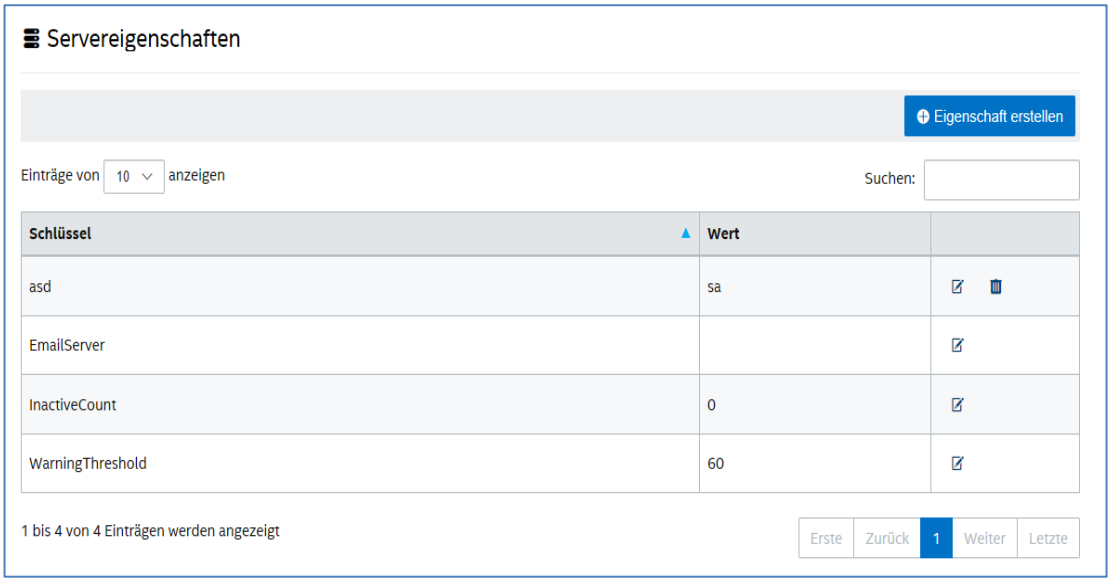


- **Servereigenschaften**: Die Schnittstelle zum Anzeigen und Ändern von Serverschlüsseln und -werten.
- **Benutzer**: Sie können jedes Konto auf dieser Seite hinzufügen, entfernen oder manuell bearbeiten.
- **Rollen**: Ermöglicht es Ihnen, neue Kategorien zu erstellen, vorhandene Rollen zu aktualisieren, Benutzerrollen zuzuweisen und Berechtigungen für die Benutzerverwaltung zu bearbeiten.
- **Moderatoren**: Mit dieser Funktion können Benutzer die Steuerung eines Meetings durch das Gruppieren von Funktionen in Rollen übernehmen, in diesem Abschnitt können Sie ganz einfach Moderatoren hinzufügen oder entfernen.
- **Reservierte PIN**: Mit dieser Funktion können IT-Administratoren bestimmten Räumen PINs zuweisen. PINs können entsprechend der stattfindenden Sitzung oder des Raumstandorts automatisch erzeugt oder manuell durch die IT eingestellt werden.
- **Telemetrie**: Zur Anzeige von Telemetriedaten muss das Telemetrie-Plugin für die Intel Unite®-Lösung installiert sein. Das Telemetrie-Plugin erlaubt IT-Administratoren Benutzerinformationen zu Intel Unite und zu den mit jedem Hub verbundenen Client-Geräten zu sammeln.

Weitere Informationen zu diesen Unterseiten finden Sie in den folgenden Abschnitten.

8.5.1 Verwaltung > Servereigenschaften

Auf dieser Seite können Sie die Schlüsselwertpaare des Servers einsehen, erstellen, bearbeiten und löschen.



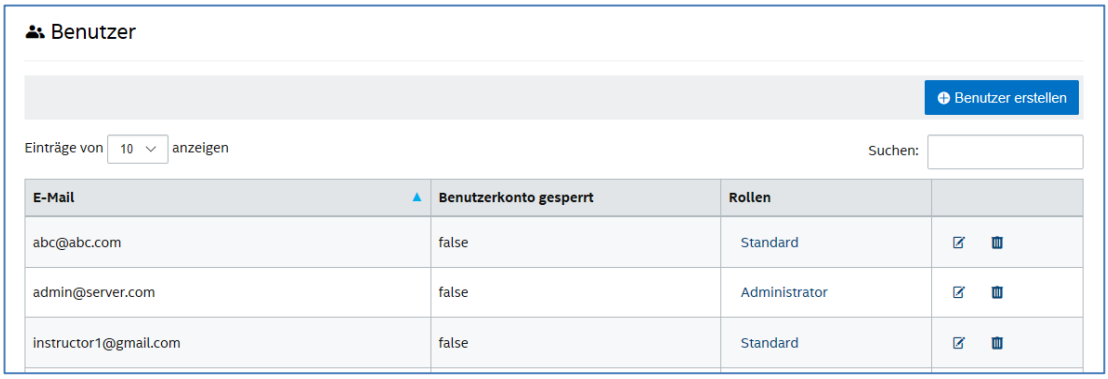
Die Schlüssel, die das Admin-Portal verwendet, lauten:

- **EmailServer**: Dies ist die E-Mail, an die der Server Benachrichtigungen sendet.
- **InactiveCount**: Wird vom Integritätsüberwachungswerkzeug der Intel Unite-Anwendung verwendet, das Benutzer E-Mails sendet, denen die Rolle Benachrichtigungen zugewiesen ist.
- **WarningThreshold**: Dient zur Bestimmung des Grenzwerts in Minuten, ab dem ein Gerät als inaktiv gilt, der Standardwert ist 60 Minuten.

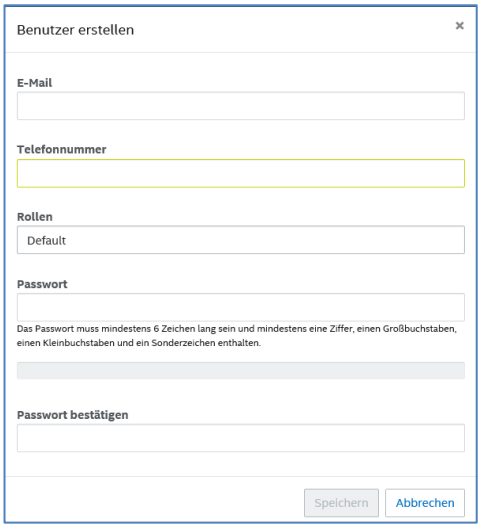
Indem Sie auf den Link **Bearbeiten** klicken, können Sie die Schlüssel entsprechend aktualisieren.

8.5.2 Verwaltung > Benutzer

Die Seite **Benutzer** zeigt eine Liste aller beim Admin-Portal registrierten Benutzer, ob ihr Konto gesperrt wurde sowie ihre Rollen an. Indem Sie auf den Link **Bearbeiten** klicken, können Sie auch diese Informationen aktualisieren.



Sie können einen neuen Benutzer hinzufügen, indem Sie auf **Benutzer erstellen** klicken und eine E-Mail-Adresse, Telefonnummer und ein Passwort eingeben. Beim Erstellen eines Benutzers können Sie auch eine bestimmte Rolle zuweisen oder den Standardwert beibehalten. Um dem neuen Benutzer Zugriffsrechte zuzuweisen, können Sie Rollen definieren und den Benutzer einer Rolle zuordnen.



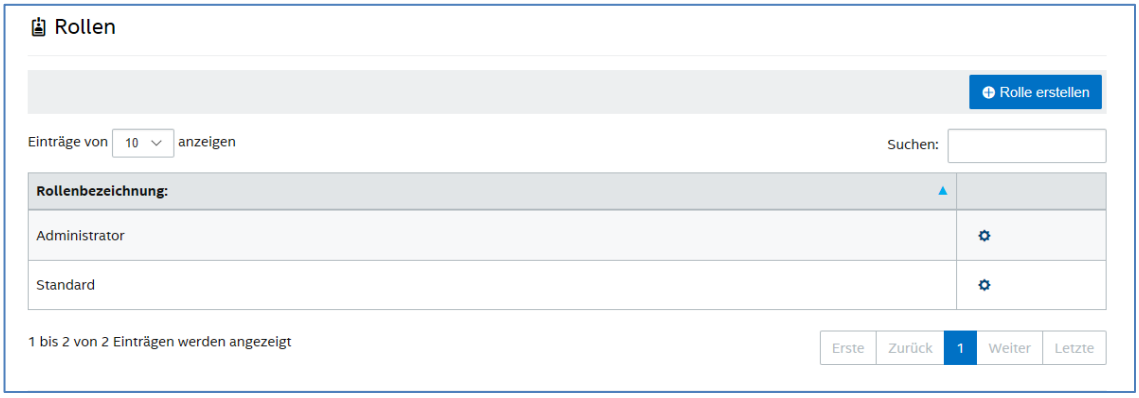
Auf der gleichen Seite können Sie durch Klicken auf die Rolle selbst (**Standard** oder **Admin**) die **Rollen** öffnen. Fahren Sie mit dem nächsten Abschnitt fort, um weitere Informationen zu **Rollen** zu erhalten.

HINWEIS zum Standardkonto: Wenn Sie ein neues Benutzerkonto hinzufügen, indem Sie sich mit dem Standardkonto admin@server.com anmelden, wird nicht automatisch eine E-Mail-Verifizierung gesendet.

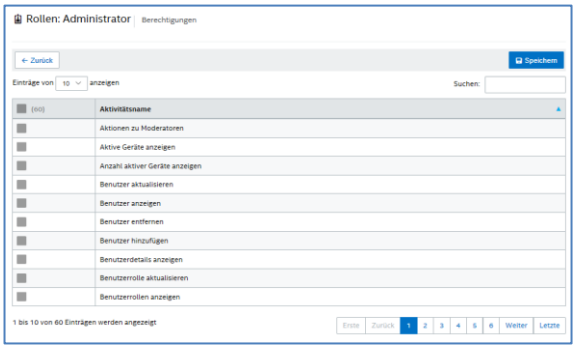
Um Ihre E-Mail-Adresse manuell zu bestätigen, loggen Sie sich mit einem neuen Konto ein, klicken Sie auf „Hallo <Ihr Benutzername>!“ in der Navigationsleiste oben rechts und klicken Sie dann auf die Schaltfläche „**Bestätigungs-E-Mail senden**“ am unteren Rand der Seite. Bevor Sie dies tun, müssen Sie die E-Mail-Einstellungen Ihres Servers in der XML-Datei „web.config“ bearbeiten. Siehe Abschnitt E-Mail-Server-Einstellungen.

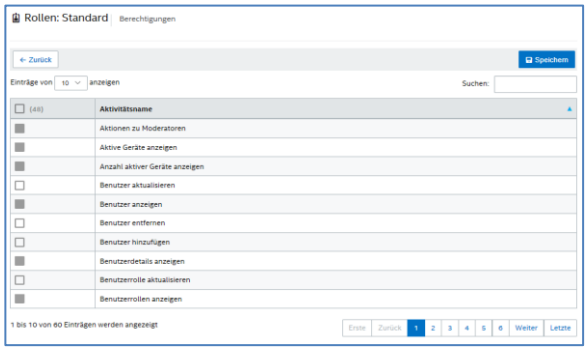
8.5.3 Verwaltung > Rollen

Diese Seite zeigt die Rollen, die derzeit definiert sind; es handelt sich um **Admin** und **Standard**. Sie können neue Rollen hinzufügen und aktuelle Rollen bearbeiten. Der Zugang zum Portal wird nicht allein durch Rollen geregelt, stattdessen sind die Aktionen auf dem Portal auf Rollen beschränkt (z. B. Erstellen eines Benutzers), die einer Reihe von Benutzern zugeordnet sind.



Klicken Sie auf das Zahnradsymbol in der rechten Spalte, um im Fenster Berechtigungen die Aktivitäten und **Berechtigungen** jeder Rolle anzuzeigen. Zugewiesene Aktivitäten können so angepasst werden, dass Sie eine Reihe von Aktionen ausführen können.





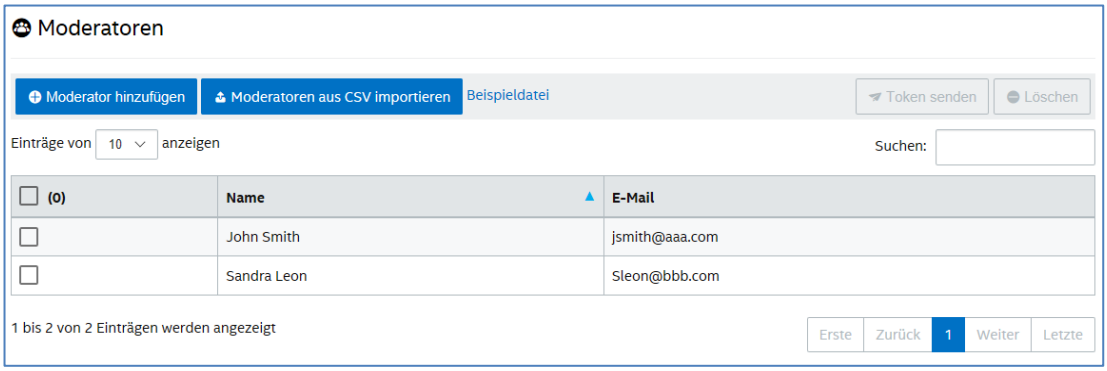
Klicken Sie auf die Schaltfläche **Rolle erstellen**, um eine neue Rolle hinzuzufügen und den Namen der Rolle zu bearbeiten. Klicken Sie dann auf der Seite **Rollen** auf das Zahnradsymbol und wählen Sie die Aktivitäten aus, die diese Rolle ausführen soll. So können Sie Berechtigungen hinzufügen oder entfernen.
Beachten Sie, dass Benutzer mehreren Rollen zugewiesen sein können.

8.5.4 Verwaltung > Moderatoren

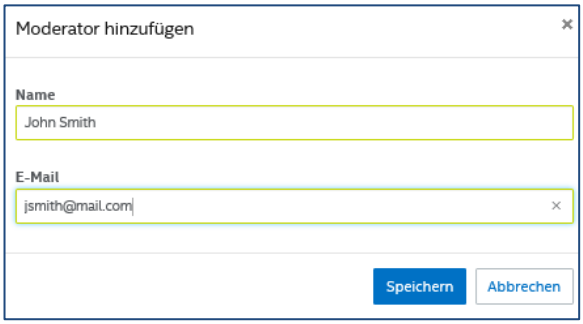
Diese Seite zeigt die Benutzer, denen die Rolle „Moderator“ zugewiesen wurde. Sie müssen einige Schritte befolgen, um einen Benutzer als Moderator hinzuzufügen.

Es gibt zwei Möglichkeiten, Moderatoren hinzuzufügen: Sie können auf **Moderator hinzufügen** klicken und die erforderlichen Daten eingeben oder Sie können durch Klicken auf **Moderatoren aus CSV importieren** eine CSV-Datei importieren, die die Namen und entsprechenden E-Mail-Adressen, die Sie zur Liste hinzufügen möchten, enthält. Stellen Sie sicher, dass Sie folgendes Format zum Import einer CSV-Datei mit dem Namen der Moderatoren verwenden: **Name,E-Mail,Aktion** oder klicken Sie auf **Beispieldatei**, um das gültigen Format anzuzeigen.

Beispiel: John Smith,jsmith@aaa.com,Hinzufügen
Sandra Leon,sleon@bbb.com,Löschen

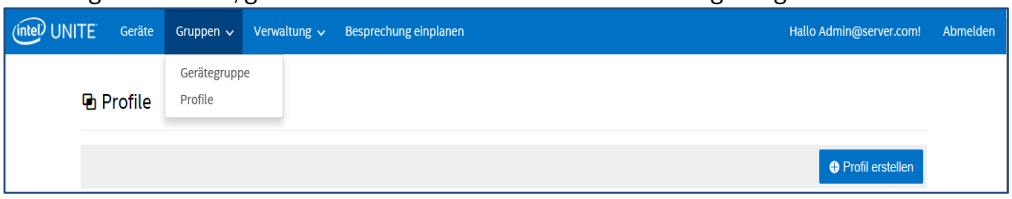


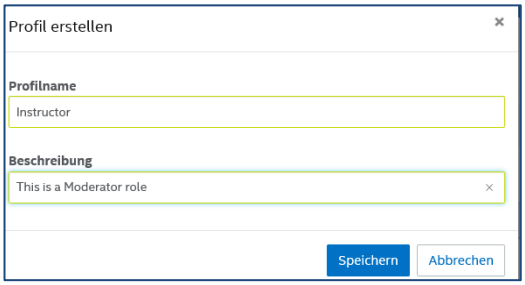
Klicken Sie auf **Moderator hinzufügen**, um **Name** und **E-Mail**-Adresse des Moderators manuell einzugeben, und klicken Sie abschließend auf **Speichern**.



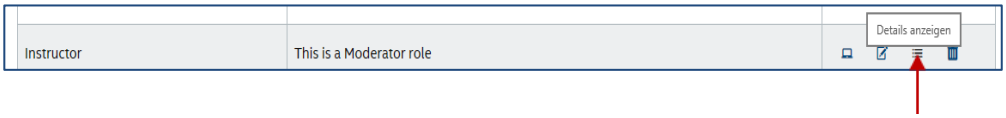
Der Modus für die Moderatorfunktion muss auf dem Profil des Hubs eingerichtet werden, Sie können auf Ihren Systemen also eine gemischte Umgebung haben. Fahren Sie mit folgenden Schritten fort:

- Gehen Sie zur Seite **Gruppen**, wählen Sie **Profile** und klicken Sie auf **Profil erstellen**. Wenn das Fenster geöffnet wird, geben Sie den Namen und die Beschreibung des gewünschten Profils ein.

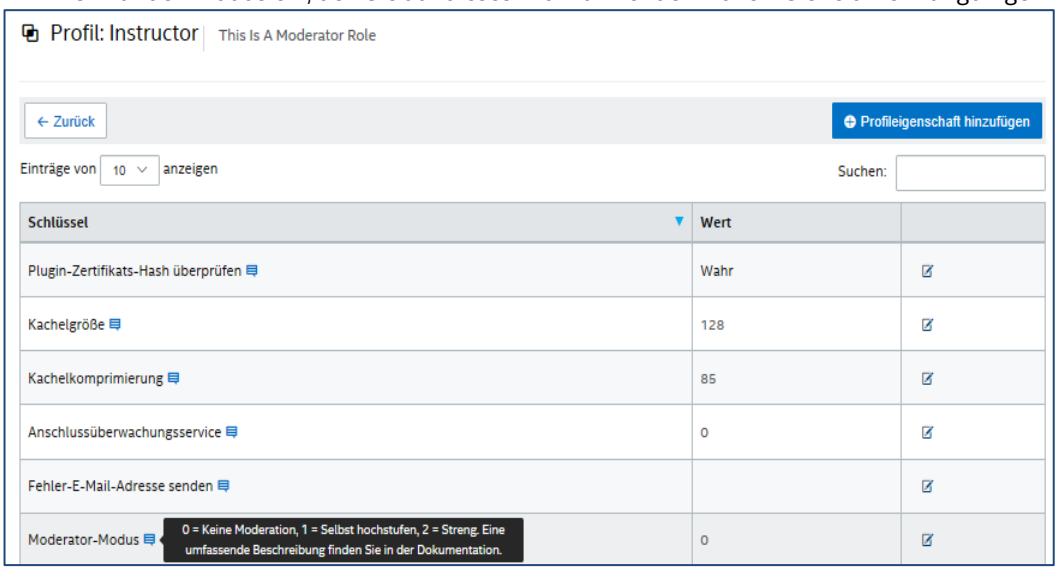




- Suchen Sie das Profil nach der Erstellung in der Liste in der rechten Spalte neben dem Profil und klicken Sie auf „Details anzeigen“.



- Suchen Sie in der Spalte **Schlüssel** nach dem **Moderatormodus** und geben Sie den gewünschten **Wert** für den Modus ein, den Sie auf dieses Profil anwenden wollen. Siehe unten für gültige Werte:



Moderatorbeschreibung und -werte:

0- **Nicht Verwaltet**: Standardmodus, kein Moderator in Meetings/Sitzungen, alle Teilnehmer haben gleiche Rechte zum Anzeigen und zur Präsentation, vorherige Intel Unite-Softwareversionen (bis v3.1) verwenden diesen Modus.

1- **Selbst Hochgestuft**: Das Meeting/die Sitzung ist nicht verwaltet, bis jemand sich selbst zum Moderator ernennt. In diesem Fall kann nur der Moderator einen weiteren Teilnehmer als Moderator bestimmen. Der Moderator kann zuweisen, wer ihn während der Sitzung vertreten soll.

2- **Streng**: Das Meeting/die Sitzung wird nur vom zugewiesenen Moderator verwaltet. Wenn ein Moderator einer Sitzung beitritt, wird dieser automatisch in diese Rolle befördert.

Hinweise:

a. Die Liste der Moderatoren wird vom IT-Administrator durch das Admin-Portal verwaltet und Moderatoren werden über einen Schlüssel authentifiziert, der ihrer E-Mail-Adresse zugeordnet ist. Bei Beförderung eines Benutzers zum Moderator sendet das Admin-Portal ihnen eine E-Mail mit einer URL, diese installiert nach Anklicken das Moderator-Token auf deren Client. Benutzer müssen diesen Prozess nur ein Mal für jedes System durchlaufen.

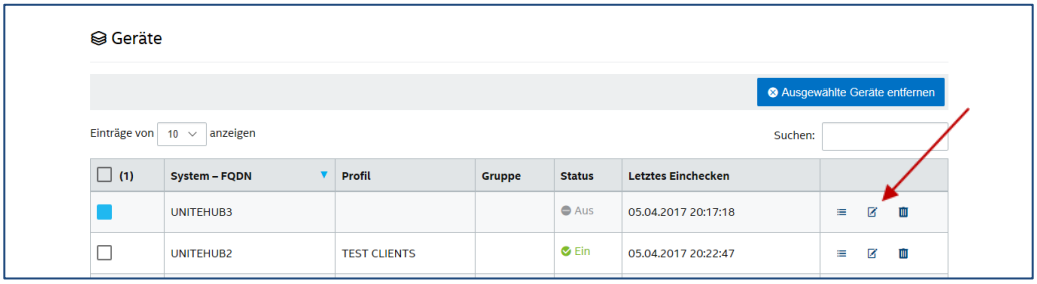
b. Der IT-Administrator kann Moderatorenrechte widerrufen, indem er das Benutzer-Token im Admin-Portal entfernt.

c. Die IT Abteilung muss zum Senden von Registrier-E-Mails an Moderatoren ein SMTP-Relais konfigurieren, damit diese Funktion ausgeführt werden kann.

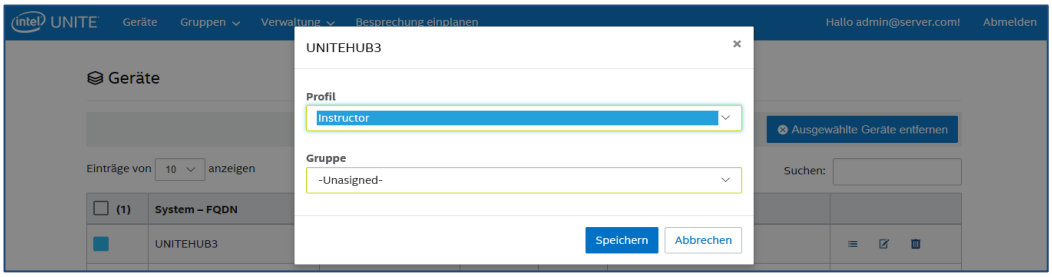
d. Wenn Sie nicht über ein SMTP-Relais verfügen und die in der E-Mail versandte URL manuell generieren müssen, gehen Sie wie folgt vor:

Gehen Sie zur Registerkarte **Verwaltung** und wählen Sie **Servereigenschaften**. Klicken Sie auf den Link **Bearbeiten** neben **EmailServer** und geben Sie das SMTP-Relais ein, Beispiel: smtp.example.com:22
Sie können nur ein SMTP-Relais konfigurieren, für das keine Authentifizierung erforderlich ist. Es ist auch möglich, das Moderator-Token abzurufen und manuell für einen Benutzer zu installieren. Im Abschnitt **Manuelle Token-Installation im strengen Modus** finden Sie weitere Details.

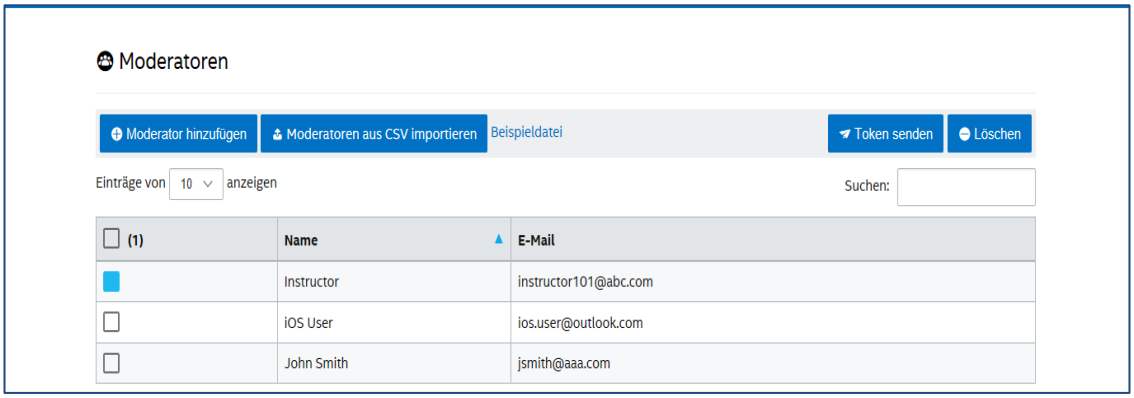
- Gehen Sie zum Aktivieren des Moderatorprofils auf einem ausgewählten Hub zur Seite **Geräte**, wählen Sie aus der Liste den zu konfigurierenden Hub und klicken Sie in der rechten Spalte auf den Link **Bearbeiten**.



- Wählen Sie, wenn das Fenster offen ist, das für den Moderator erstellte Profil in Abschnitt „Profil“ sowie gegebenenfalls die Gruppe, in die dieser gehört, und **Speichern** Sie dann.



Sobald Sie die Liste der Moderatoren ausgefüllt haben, können diese durch Auswahl (blauer Rahmen) und Klicken auf **Löschen** gelöscht werden. Wählen Sie den Namen und klicken Sie auf **Token senden**, um dem Moderator eine URL für die Teilnahme an einem Meeting/einer Sitzung zu senden.



8.5.4.1 Manuelle Token-Installation im strengen Modus

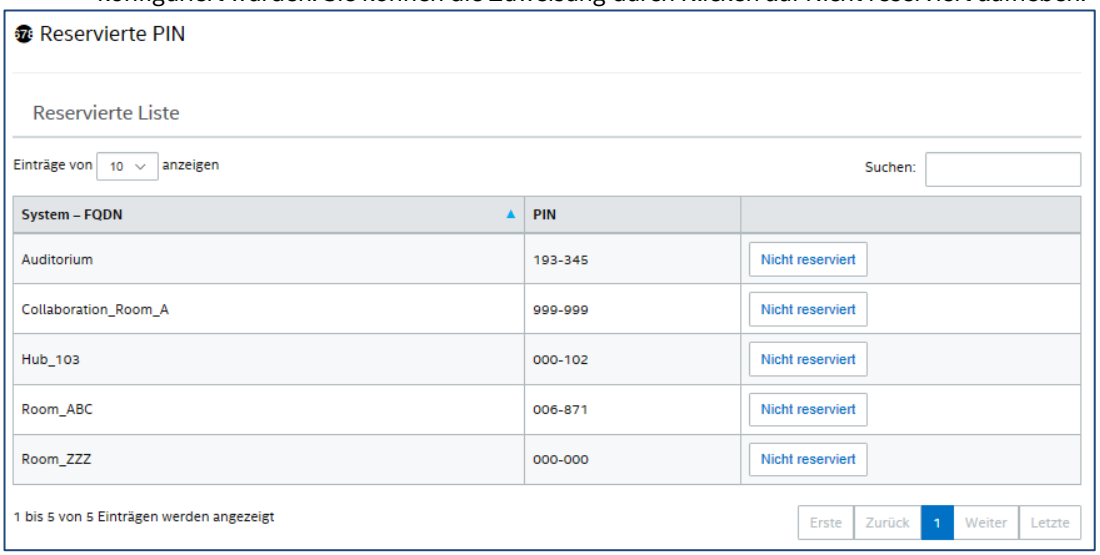
Wenn Sie kein SMTP-Relais haben, können Sie das Moderator-Token abrufen und manuell für einen Benutzer installieren, der als Moderator hinzugefügt wurde. Dazu muss Microsoft SQL Server Management Studio installiert sein.
Abrufen des Token:

- Fügen Sie einen Moderator hinzu
- Öffnen Sie Microsoft SQL Server Management Studio und stellen Sie unter Verwendung der Admin-Anmeldedaten, die während der Installation des Enterprise-Servers verwendet wurden, eine Verbindung zum Datenbankserver her
- Erweitern Sie „Datenbanken“, dann „UniteServer“ und dann „Tabellen“
- Klicken Sie mit der rechten Maustaste auf „dbo.Moderators” und dann auf „Oberste 1000 auswählen“
- Suchen Sie in den Ergebnissen nach dem „Benutzernamen“ der mit dem übereinstimmt, den Sie im vorherigen Schritt hinzugefügt haben
- Klicken Sie mit der rechten Maustaste und kopieren Sie das Token in die Zwischenablage
- Öffnen Sie den Editor und erstellen Sie die URL: intelunite://localhost/SetModerationToken?Token=<Token aus dem vorherigen Schritt einfügen>
- Öffnen Sie Intel Unite
- Auf Windows-Geräten: Öffnen Sie den Explorer, kopieren Sie die vollständige URL, fügen Sie sie ein und drücken Sie die Eingabetaste
- Auf Mac-Geräten: Öffnen Sie Safari, kopieren Sie die vollständige URL, fügen Sie sie ein und drücken Sie die Eingabetaste

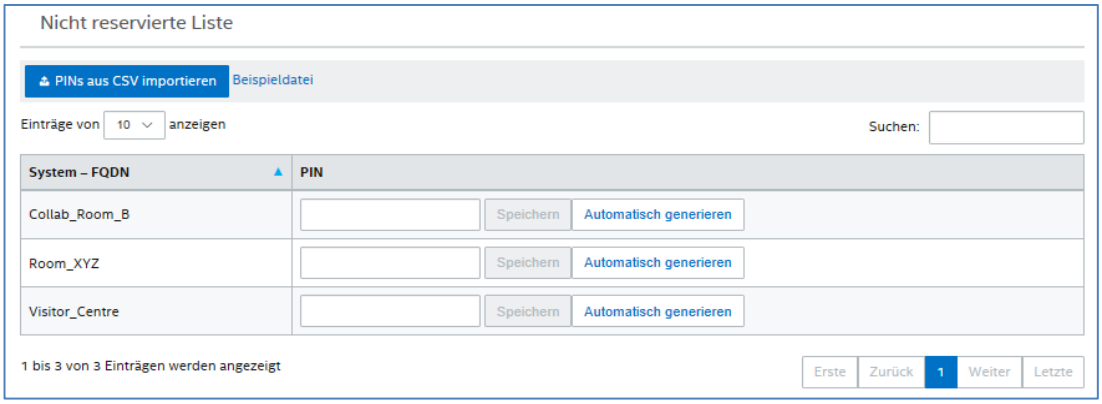
8.5.5 Verwaltung > Reservierte PIN

Diese Seite zeigt zwei Bereiche an, die **Reservierte Liste** und die **Nicht reservierte Liste** der Systeme, in denen die PIN während der Meetings/Sitzungen statisch ist oder nicht. Der IT-Administrator kann Systeme in ausgewählten Räume zuweisen, in denen Benutzer während des Meeting oder der Sitzung dieselbe PIN eingeben oder eine wechselnde PIN mit dem Standardwert.

- **Reservierte Liste** – Dabei handelt es sich um die Liste der Reservierungen, die bereits durch die IT konfiguriert wurden. Sie können die Zuweisung durch Klicken auf Nicht reserviert aufheben.



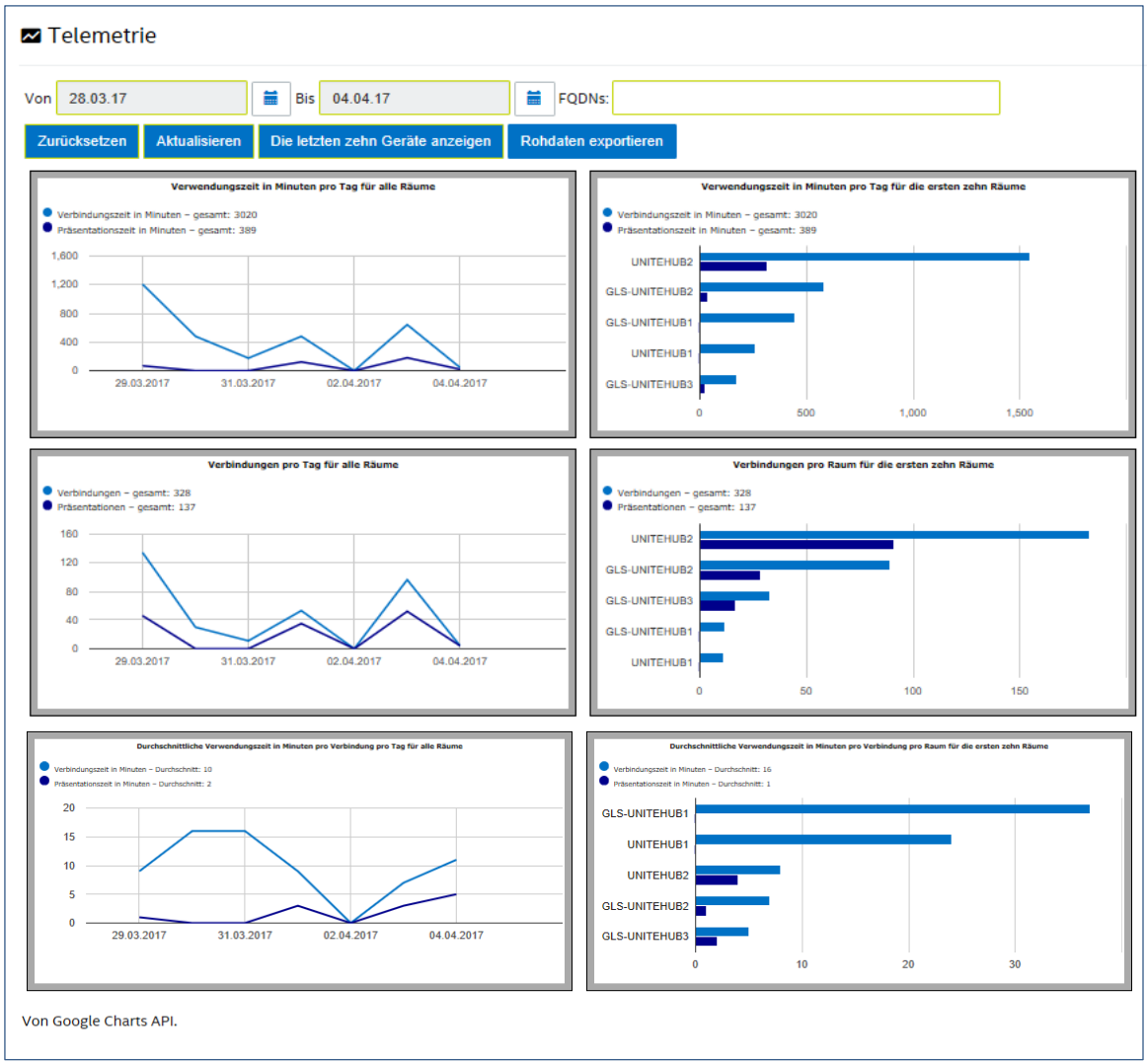
- **Nicht reservierte Liste** – Dabei handelt es sich um die Liste der Systeme, die keine statischen PIN-Reservierungen haben. PINs können manuell eingegeben, automatisch erstellt oder aus einer CSV-Datei importiert werden.



Klicken Sie bei der Zuweisung von PINs auf Speichern, um die Werte beizubehalten.

8.5.6 Verwaltung > Telemetrie

Diese Seite zeigt Telemetriedaten, die durch das Admin-Portal erfasst wurden. Zur Anzeige dieser Daten muss das Telemetrie-Plugin für die Intel Unite®-Lösung installiert sein. Das Telemetrie-Plugin erlaubt IT-Administratoren Benutzerinformationen zu Intel Unite und zu den mit jedem Hub verbundenen Client-Geräten zu sammeln. Den IT-Administratoren werden Informationen wie die Anzahl der Verbindungen pro Raum, die Verbindungen am Tag, durchschnittliche Verbindungszeit usw. angezeigt. Bitte lesen Sie das **Intel Unite® Plugin für Telemetrie-Benutzerhandbuch** für ausführliche Informationen und die Bereitstellung des Plugins in Ihrem System.



8.6 Seite „Besprechung einplanen“

Sie Seite „Besprechung einplanen“ ist eine Funktion, die eine Sitzungs-URL für Sitzungsteilnehmer erstellt, die das vorhandene Intel Unite-Plugin für Microsoft Office nicht installieren oder verwenden können. Alle Teilnehmer können diese Seite anzeigen.

Klicken Sie einfach auf die Schaltfläche **Neue Besprechung erstellen**, um die URL zu erstellen und diese den Benutzern zu senden, die an dem Meeting oder der Sitzung teilnehmen.

8.7 Andere Konfigurationsoptionen für das Admin-Portal

8.7.1 Profilkonfiguration

Profile können konfiguriert werden, indem Sie auf **Gruppen** > **Profile** zugreifen und auf **Details** des Profils im Admin-Portal klicken. Dadurch werden die Konfigurationseinstellungen in der Form eines „Schlüssel-Wert“-Paares angezeigt. Sie können die Werte ändern, um die Anwendung anzupassen und die Benutzererfahrung des Meeting-/Sitzungsraums anzupassen. Zu den Einstellungen, die Sie ändern können, gehören zum Beispiel: Hintergrundbilder der Hub-Anzeige, PIN-Größe, Schriftfarbe und Inhalt.
Nachdem Sie die Werte eines Profils angepasst haben, weisen Sie den Profilen Geräte zu, um die Profileinstellungen anzuwenden. Klicken Sie auf **Geräte anzeigen** und dann auf **Geräteliste aktualisieren**, um das Profil auf Geräte anzuwenden. Die Geräteliste wird Ihnen angezeigt; klicken Sie auf das Kontrollkästchen neben dem Gerät, um die Konfigurationseinstellungen anzuwenden.

In der untenstehenden Tabelle sind verfügbare **Schlüssel**, ihre Beschreibung, der Datentyp sowie die Standardwerte der Schlüssel aufgeführt.

Schlüssel	Beschreibung	Datentyp	Standardwert
Datei-Übertragung erlauben	Kennzeichen, das die Übertragung einer Datei durch einen Hub oder Client aktiviert/deaktiviert	Boolesche Datentypen	Falsch
Support für Audio-/Video-Streaming	Kennzeichen, dass Windowsbenutzern die Möglichkeit gibt, ihren Desktop mit dem vollen A/V-Erlebnis (1080p bei 20-30fps) zu präsentieren	Boolesche Datentypen	Wahr

PIN während Besprechung ändern	Sperren Sie die PIN für ein Meeting/eine Sitzung, die PIN bleibt unverändert, bis alle Benutzer sich abmelden Wahr = PIN kann während der Sitzung geändert werden Falsch = PIN während der Sitzung sperren	Boolesche Datentypen	Wahr
Remote-Ansicht deaktivieren	Deaktivieren der Remote-Ansicht aus bestimmten Räumen. Bei Aktivierung wird einem Benutzer, der Inhalte über die Remote-Ansicht anzeigen will, ein Hinweis angezeigt, dass diese Funktion nicht verfügbar ist Wahr = Deaktiviert Remote-Ansicht Falsch = Erlaubt Remote-Ansicht	Boolesche Datentypen	Falsch
Größe der PIN anzeigen	Größe in Pixeln. Der Wert entspricht der Höhe in Pixeln von PINs auf dem Bildschirm (je größer der Wert, desto leichter ist es, PINs aus der Ferne lesen zu können)	Integer	48
Transparenz für PIN-Anzeige	Steuert die Alpha-Transparenz der auf dem Bildschirm angezeigten PIN 100 = 100 % sichtbar 1–99 = PIN ist mit einem Rahmen sichtbar, die Opazität ändert sich je nach verwendetem Wert 0 = Die PIN ist transparent	Integer	100
Datei blockierte Erweiterungen, Anzeige als blockierte Dateierweiterungen	Komma-getrennte Liste der blockierten Dateierweiterungen (z. B. exe, bin, msi)	Zeichenkette	Leeres Feld
Datei maximale Größe Anzeige als maximale Dateigröße	Max. Dateigröße für Dateiübertragungen	Integer	2147483647 Byte (zulässiger Bereich: 0 bis 2147483647)
Vollbildmodus	Hub-Vollbild aktivieren/deaktivieren Falsch: PIN nur oben rechts Wahr: PIN oben rechts und Hintergrund des Vollbildes	Boolesche Datentypen	Falsch
Hintergrundfarbe Vollbildmodus	Im Hub verwendete Hintergrundfarbe. HTML-Farben (Hexadezimale Farben). Beispiele für gültige Werte (RGB-Werte, Format #000000) sind: Rot: #FF0000 Gelb: #FFFF00 Grün: #00FF00 Hellblau: #00FFFF Dunkelblau: #0000FF Schwarz: #000000 Weiß: #FFFFFF Grau: #808080	Zeichenkette	Leeres Feld (wird in Schwarz angezeigt)

Vollbildmodus – Hintergrundbildstreckung	Kennzeichen, um das Hintergrundbild über den gesamten Bildschirm zu strecken	Boolesche Datentypen	Falsch
Vollbildmodus - Hintergrundfarbe-URL	Legt Hub-Hintergrund auf angegebene URL oder angegebenes Bild (JPG/PNG) fest. Wert als True festlegen, wenn diese Funktion aktiviert werden soll Beispiel: http://myserver.com/background.jpg	Zeichenkette	Leeres Feld
Vollbildmodus - Anweisungen	Textanweisungen werden auf dem Hub angezeigt. {pin} und {host} können zum Ersetzen verwendet werden URL zum Download des Clients Dieses Element wird im Vollbildmodus angezeigt.	Zeichenkette	{pin}
Vollbildmodus - Pinfarbe	Farbe der angezeigten PIN	Zeichenkette	Leeres Feld (wird in Weiß angezeigt)
Vollbildmodus - Pin anzeigen	Anleitungen anzeigen. Wert als True festlegen, wenn diese Funktion aktiviert werden soll	Boolesche Datentypen	Falsch
Vollbildmodus - Schriftfarbe	Farbe des auf dem Hub angezeigten Texts	Zeichenkette	Leeres Feld (wird in Weiß angezeigt)
Vollbildmodus - Schriftart	Schriftart für Anweisungen	Zeichenkette	Leeres Feld
Hub - Tastatur sperren	Das Folgende ausschließen: Strg-Esc, Alt-Tab, Charms-Leiste, Windowstaste und Alt-F4 in Hub Hub wird ausgeschlossen, wenn als „wahr“ festgelegt. Kann mit Passwort in Reg Key Machine außer Kraft gesetzt werden (REG KEY-Wert)	Boolesche Datentypen	Falsch
Hub - Uhr anzeigen	Uhrzeit in unterer rechter Ecke anzeigen	Boolesche Datentypen	Wahr
Moderator-Modus	Verwenden Sie für die Zuweisung des Moderatormodus für Meetings/Sitzungen folgende Werte: 0 = Keine Moderation 1 = Selbstanwendung 2 = Streng	Integer	0
Fehler-E-Mail-Adresse senden	Zuweisen einer E-Mail-Adresse, an die der Hub Fehlermeldungen sendet	Zeichenkette	Leeres Feld (wird in Weiß angezeigt)
Anschlussüberwachungsservice	Ein Port, über den der Hub eingehende Verbindungen abruft	Integer	0 (0 = Auto-adressierter Port)

Kachelkomprimierung	Hiermit kann das Komprimierungsverhältnis für die Freigabe von Nicht-AV-Inhalten eingestellt werden. Komprimierung in %, die auf einen geänderten Abschnitt des Displays (Kachel) angewendet werden soll, der über das Netzwerk übertragen wird (Höherer Wert benötigt mehr Bandbreite)	Integer	85 (zulässiger Bereich: 5 bis 100)
Kachelgröße	Damit kann die Kachelgröße für die Freigabe von Nicht-AV-Inhalten eingestellt werden. Kachelgröße, wenn Bildschirm in Blöcke aufgeteilt wird. Größe in Pixeln pro Kachel.	Integer	128 (zulässiger Bereich: 32 bis 512)
Plugin-Zertifikats-Hash überprüfen	Plugins benötigen Überprüfung Wahr = Zertifikat-Hashwert überprüfen Falsch = Zertifikat-Hashwert nicht überprüfen	Boolesche Datentypen	Wahr

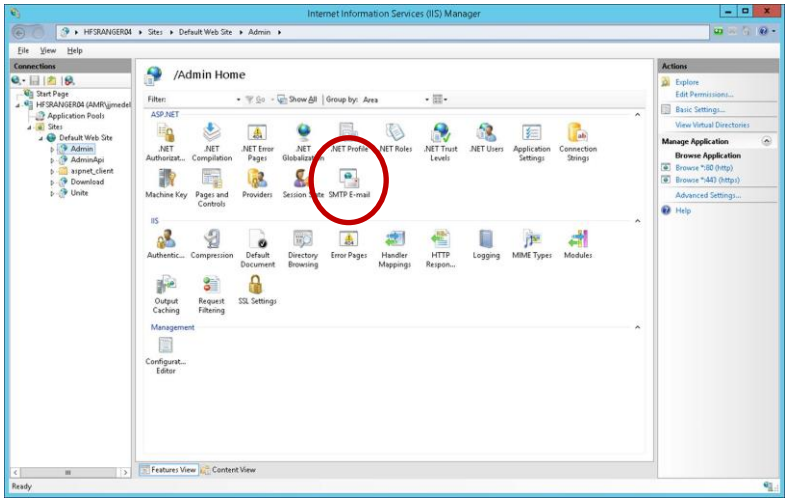
8.7.2 Aktualisierungsintervall der PIN

Das Aktualisierungsintervall der PIN beträgt 5 Minuten, d.h. der auf dem Hub angezeigte PIN ändert sich alle 5 Minuten. Dies kann in 1-Minuten-Schritten zu Intervallen von 2 bis 60 Minuten geändert werden. Dazu muss die Datei **web.config** im Stamm des virtuellen Verzeichnisses der Webdienst-Website geändert werden. Der Zugriff erfolgt über den IIS-Manager. Auf die Datei kann außerdem zugegriffen werden, indem Sie zum Verzeichnis Intel Unite\PinServer navigieren. Das Verzeichnis ist standardmäßig unter C:\Programmdateien (x86)\Intel\Intel Unite\PinServer installiert.
Stellen Sie den Wert unter dem Tag <add key="**PinExpireTimeInMinutes**" value="5"></add> auf das gewünschte Aktualisierungsintervall um.

8.7.3 E-Mail-Server-Einstellungen

Das Admin-Portal definiert den SMTP-Server in der xml-Datei „web.config“, die bei der Installation der Intel Unite Anwendung auf dem Server erstellt wird. Je nachdem, wo Ihr SMTP-Server konfiguriert wird, müssen die **mailSettings** in der xml-Datei „web.config“ so modifiziert werden, dass „host“ auf Ihren SMTP-Server ausgerichtet ist. (Die xml-Datei „Web.config“ befindet sich standardmäßig unter C:\Programmdateien (x86)\Intel\Intel Unite\PinServer).
Sicherstellen, dass der SMTP-e-Server unter IIS konfiguriert wurde und dass die Einstellung korrekt ist, um mit der Anwendung während der Vorinstallation des Enterprise-Servers zu arbeiten.
Die Datei-Einstellungen sehen wie folgt aus:

```
<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 Warnmeldungen und Überwachung

Der Enterprise-Server bietet Warn- und Überwachungsdienste an. Dieser Dienst muss eingerichtet und im Admin-Portal konfiguriert werden.
Jedes Gerät, für das Warnmeldungen eingerichtet sind, wird überwacht. Wird der Warnungsschwellenwert überschritten, wird eine E-Mail an die angegebenen Benutzer gesendet.
Wenn Sie über inaktive Geräte per E-Mail benachrichtigt werden möchten, muss die Rolle **Notifications** dem Benutzer im Admin-Portal zugewiesen sein. Wenn Sie die Überwachung eines Geräts einrichten möchten, fügen Sie den Schlüssel **EnableReporting** zu dessen Metadaten hinzu und setzen Sie den Wert auf **wahr**.
Der Warnungsschwellenwert wird in **Verwaltung** > **Server-Eigenschaften** konfiguriert. Sein Standardwert beträgt 60 Minuten.
InactiveCount: Wenn der Benutzer bei der nächsten Prüfung sofort benachrichtigt werden möchte, muss der Wert entsprechend niedrig eingestellt werden.
Die E-Mail-Adresse (smtp from) und der E-Mail-Server (host) muss in der Datei **clocktower.exe.config** angegeben werden. Sie befindet sich unter: /productfiles/release/clocktower.exe.config. (Die xml-Konfigurationsdatei „clocktower.exe“ befindet sich standardmäßig unter C:\Programmdateien (x86)\Intel\Intel Unite\ClockTower).

Die Datei-Einstellungen sehen wie folgt aus:

```
<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 Sicherheitskontrollen für Betriebssystem und PC

9.1.1 Mindest-Sicherheitsstandards (MSS)

Es wird empfohlen, dass alle Geräte, die die Intel Unite Anwendung verwenden, die MSS-Standards Ihres Unternehmens einhalten. Auf den Geräten sollte ebenfalls ein Patch-Agent, eine Antivirus-/IPS-/IDS-Software installiert und andere Kontrollen aktiviert sein, die in den MSS-Standards vorgesehen sind (McAfee-Suite als Anti-Malware-, IPS- und IDS-Software wurde auf Kompatibilität getestet).

9.1.2 Computer härten

Die „Machine Unified Extensible Firmware Interface“ (vereinheitlichte erweiterbare Firmware-Schnittstelle, UEFI) kann gesperrt werden, um nur das Windows-Startladeprogramm zu starten (das Starten von einer USB-Festplatte oder einer DVD funktioniert nicht), die Funktion „Execute Disable Bit“ kann aktiviert werden, die Intel® Trusted Execution Technik kann aktiviert und deren Einstellungen mit einem Passwort geschützt werden.

Windows Betriebssystem härten: Das System läuft ohne erhöhte Benutzerrechte. Es wird empfohlen, nicht genutzte Software, einschließlich nicht benötigter, vorinstallierter Software und Windows-Komponenten zu entfernen (PowerShell, Druck- und Dokumentdienste, Windows-Positionssuche, XPS-Dienste).

GUI-Subsystem sperren: Da das System ein Non-Touch-Display ohne Tastatur und Maus verwendet, ist es schwerer aus dem GUI-Subsystem auszubrechen. Um zu verhindern, dass ein Angreifer auf ein HID-Gerät zugreifen kann (US-Tastatur/Maus), wird empfohlen, programmatisch **Alt+Tab**, **Strg+Umschalttaste+Esc** sowie die **Charms**-Leiste zu sperren.

9.1.3 Andere Sicherheitskontrollen

Es wird empfohlen, das Benutzerkonto über das entsprechende Computerkonto in „Active Directory“ zu sperren. Wenn die Anwendung viele Einheiten enthält, können Benutzerkonten über ein Stockwerk eines bestimmten Bauplans gesperrt werden.

Besitz des Computers: Es wird empfohlen, für jeden Computer einen Besitzer anzugeben. Wird der Computer für längere Zeit offline geschaltet, wird der Besitzer benachrichtigt.
Neben den eigenen Sicherheitsmechanismen der Intel vPro Plattform und der Intel Unite Software wird eine Härtung des Windows-Betriebssystems gemäß den Microsoft-Richtlinien zum Härten von Computern empfohlen. Informationen hierzu finden Sie im Microsoft Security Compliance Manager* (SCM) unter dem folgenden Link: https://technet.microsoft.com/en-us/solutionaccelerators/cc835245.aspx
Hinweis: Die über diesen Link bereitgestellten Informationen umfassen ein Assistent-gestütztes Härtungs-Tool, einschließlich Härtung nach bestem Verfahren sowie mit relevanter Dokumentation.

10 Wartung

Ihre Organisation und Ihr IT-Administrator werden ein regelmäßiges Wartungsprogramm einrichten. Die folgenden Wartungsarbeiten werden empfohlen:

10.1 Nächtlicher Neustart

Es wird empfohlen, den Computer täglich neu zu starten (bevorzugt über Nacht). Vor diesem Neustart sollten Wartungsaufgaben ausgeführt werden, wie beispielsweise das Löschen zwischengespeicherter temporärer Dateien und die Einleitung des standardmäßigen Patch-Vorgangs.

10.2 Patch-Strategie

Führen Sie den Patch-Vorgang, falls möglich, in einem unbeaufsichtigten Modus aus (keine GUI-Befehle), bevorzugt vor dem zuvor erwähnten Neustart.

10.3 Berichterstattung

Erfassen Sie die Anzeigen der Zeit, in der Ihr Computer in Betrieb ist, und erstellen Sie einen genauen Bericht über den Bedarf Ihres Unternehmens.

10.4 Überwachung

Nutzen Sie ein Systemüberwachungstool, das die Leistung des Computers überwacht und führen Sie Back-End-Analysen über Betriebszeiten durch.

10.4.1 Back-End-Überwachung:

Nutzen Sie virtuelle Überwachungstools, um Warnmeldungen zu erzeugen und an den Second-Level-Support zu schicken.

11 Intel Unite-Lösung für macOS

11.1 Hintergrund

Die Intel Unite Software für macOS ist als Primär-App-Paket verpackt und kann spezifische IT-Präferenzwerte nutzen. Auf diese Weise wird ermöglicht, dass die App eine Vielzahl an allgemeinen Bereitstellungen unterstützt, wie beispielsweise allgemeine Mac-Verwaltungssoftware und -techniken oder die manuelle Installation und Einstellung von Präferenzen.

11.2 Allgemeiner Verbindungs-Workflow

Die App verwendet standardmäßig „DNS Auto Discovery“ (z. B. DNS-SRV-Einträge), um sich mit dem eigenen Enterprise-Server zu verbinden. Der Workflow läuft insgesamt gesehen folgendermaßen ab:

- (Optional) Enterprise-Server je nach Definitionen in den Präferenzen
- Auto Discovery für folgende Domains:
  - _uniteservice._tcp
  - _uniteservice._tcp.yourSubDomain.yourDomain.yourTLD
    i. Beispiel: _uniteservice._tcp.corp.acme.com
  - _uniteservice._tcp.yourDomain.yourTLD
    i. Beispiel: _uniteservice._tcp.acme.com
  - Versuch des Verbindungsaufbaus über HTTPS und dann über HTTP, falls Verbindungsaufbau erfolglos
- uniteservice.yourDomain.yourTLD

11.3 Präferenzwerte

Über IT kann die Intel Unite App modifiziert und angepasst werden, damit eigene Bedürfnisse an Infrastruktur und Sicherheit erfüllt werden können. Dazu müssen folgende Einstellungen für „com.intel.Intel-Unite.plist“ vorgenommen werden (im Ordner ~/Bibliothek/Präferenzen jedes Benutzers):

- **Definieren Sie einen Enterprise-Server als Standard.**
  defaults write com.intel.Intel-Unite EnterpriseServer myServer.mydomain.myTLD

- **Legen Sie einen Enterprise-Server Public Key für Certificate Pinning fest.**
  defaults write com.intel.Intel-Unite EnterpriseServerPublicKey "Public Key String"

- **Schreiben Sie „Only Allow Trusted Server Certificates“ („nur vertrauenswürdige Serverzertifikate zulassen“) für Clients vor.**
  defaults write com.intel.Intel-Unite ClientOnlyAllowsTrustedCertificates -bool true

- **Schreiben Sie „Connect in Standalone Mode“ („im eigenständigen Modus verbinden“) für Clients vor.**
  defaults write com.intel.Intel-Unite Standalone -bool true

Jede dieser Einstellungen kann manuell vorgenommen oder geändert werden, indem Sie das macOS-Terminal (/Anwendungen/Dienstprogramme) öffnen und den Befehl gefolgt von der Eingabetaste eingeben. Dialog und Details für jeden Befehl sehen folgendermaßen aus:

- **Definieren Sie einen Enterprise-Server als Standard.**
  Durch das Festlegen eines Enterprise-Servers als Standard wird der Auto-Discovery-Prozess angehalten. Wenn Ihren Mac-Clients nur dieses eine Netzwerk zur Verfügung steht, kann es

nützlich sein, die Intel Unite App aus Sicherheitsgründen oder zur Problembehebung an Ihren Enterprise-Server anzuheften.

- **Legen Sie einen Enterprise-Server Public Key für Certificate Pinning fest.**
  Wenn Sie die Client-Anwendung an Ihren Enterprise-Server anheften möchten – unabhängig davon, ob Auto-Discovery verwendet wird oder nicht – können Sie für jeden Client einen „Public Key String“ einrichten. Um den Wert zu erhalten:
  - Öffnen Sie Safari auf einem beliebigen Mac-Gerät in Ihrem Unternehmensnetzwerk.
  - Gehen Sie zur HTTPS-Adresse Ihres Enterprise-Servers.
  - Klicken Sie auf das Sperrsymbol in der Adressleiste.
  - Klicken Sie auf der Zertifikatseite auf die Schaltfläche **Zertifikat anzeigen**.
  - Klicken Sie auf das Dreiecksymbol **Details** um die Information offenzulegen und die Anzeige zu erweitern.
  - Scrollen Sie durch die Zertifikatdaten, bis Sie das Feld **Public Key Info** > **Public Key** finden.
  - Klicken Sie auf das Datenfeld, das mit „256 Byte:“ beginnt.
  - Das Datenfeld wird erweitert.
  - Wählen Sie mit der Maus oder mit CMD+A alle Daten im Feld aus.
  - Kopieren Sie die Daten in Ihre Zwischenablage, indem Sie **Kopieren** aus dem Kontextmenü oder **CMD+C** verwenden.
  - Ersetzen Sie im Standardbefehl den **Public Key String** durch die Daten aus der Zwischenablage. Hinweis: Sie müssen die Daten in doppelte Anführungsstriche einschließen.

  Durch das Einrichten dieser Option wird es – in ähnlichem Maße wie beim Definieren eines Enterprise-Servers als Standard – Ihrer Benutzerschaft deutlich erschwert, sich mit anderen Intel Unite Installationen anderer Partner/Standorte zu verbinden.

- **Schreiben Sie „Only Allow Trusted Server Certificates“ („nur vertrauenswürdige Serverzertifikate zulassen“) für Clients vor.**
  Zusätzlich zum Definieren eines spezifischen Enterprise-Servers und das Anheften des Public Keys des Zertifikats, können Sie außerdem die Intel Unite App so konfigurieren, dass sie nur Verbindungen zu Servern/Zertifikaten zulässt, die gemäß Ihrer Zertifikatvertrauenskette zulässig sind. Dabei müssen Sie sicherstellen, dass das Zertifikat Ihres Enterprise-Servers gemäß der Definition von Apple in der Keychain wieder zurück an einen öffentlichen Stammserver geleitet wird oder, dass Sie Ihr eigenes Stammserverzertifikat sowie alle für jeden Client erforderlichen Zwischenzertifikate installiert haben.

- **Schreiben Sie „Connect in Standalone Mode“ („im eigenständigen Modus verbinden“) für Clients vor.**
  Durch Einrichten dieses Modus wird der Verbindungs-Workflow geändert und eine UDP-Auto-Discovery eines Hubs durchgeführt, der eine PIN in einer Umgebung ohne Enterprise-Server erzeugt hat. In diesem Szenario agiert das auf dem Intel vPro Prozessor basierende System als Primärhost. Dies bietet sich vor allem für Umgebungen kleinerer und mittlerer Unternehmen an, in denen es unter Umständen keine IT-Abteilung gibt, die die Enterprise-Server-Struktur installieren kann. Dieser Modus funktioniert nur systemübergreifend innerhalb desselben Subnetzes, wenn UDP-Pakete nicht blockiert werden.

11.4 Häufige Verteilungsmethode

Beim Verwenden von Auto Discovery kann die Intel Unite Anwendung ganz einfach durch Ziehen in den Anwendungsordner verteilt werden. In komplexeren Umgebungen oder Umgebungen, die zusätzliche Sicherheitseinstellungen benötigen, sollten zur Verteilung des App-Pakets spezifische Präferenzen eingerichtet werden. Dazu gibt es zahlreiche Methoden; im Folgenden haben wir die häufigsten für Sie zusammengefasst:

- Bash-Skript

- Sie können Ihre Präferenzen in einem Bash-Skript definieren, das an Benutzer in Verbindung mit dem App-Paket verteilt werden kann.

- Benutzerdefiniertes Installationspaket über PackageMaker
  - Sie können Ihre Präferenzen über ein Pre- oder Postflight-Skript definieren.
- Benutzerdefiniertes Installationspaket über Apple Remote Desktop
  - Mit Apple Remote Desktop können Sie das Intel Unite App-Paket installieren und alle Präferenzen über das Menü **UNIX-Befehl senden...** definieren.
- Benutzerdefiniertes Installationspaket über Enterprise Mac Management Software
  - Mit den am häufigsten verwendeten Enterprise Mac Management Lösungen lassen sich benutzerdefinierte Push-oder-Pull-Installationen erstellen, u.a.:
    - Casper/Bushel
    - Puppet
    - Munki
    - Chef
    - Etc.

12 Fehlerbehebung

12.1 Die Admin-Portalseite ist nach der Installation der Intel Unite Anwendung auf dem Server nicht erreichbar.

Umgehung/Lösung: Stellen Sie sicher, dass die erforderlichen Rollen und Funktionen für Web-Server dem Server hinzugefügt wurden.

- Fügen Sie mit dem Server-Manager dem Server Rollen und Funktionen hinzu.
    - Server-Rollen: Web-Server
        - Verwaltungstools einschließen.
    - Funktionen für .NET Framework 3.5 hinzufügen.
    - Funktionen für .NET Framework 4 hinzufügen.
        - ASP .NET
            - WCF-Dienste
            - HTTP-Aktivierung
        - Web-Server-Rollen:
            - Web-Server, allgemeine HTTP-Funktionen und Standarddokument.

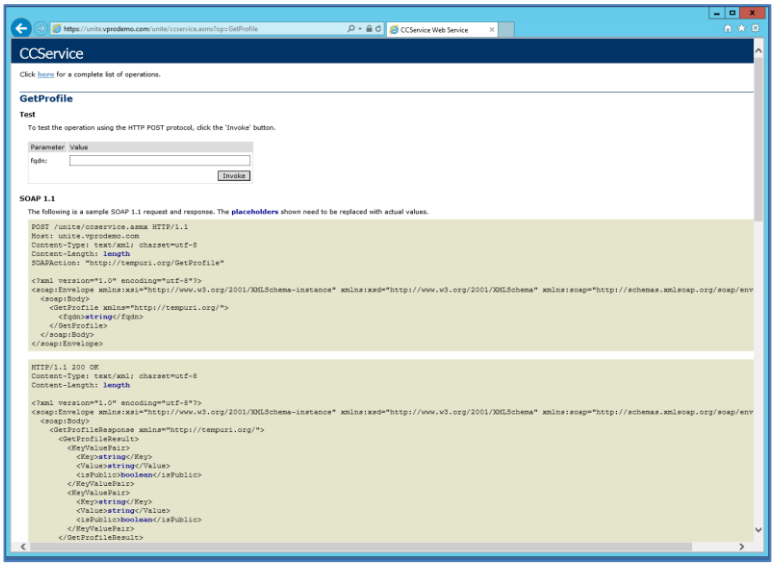
12.2 Kein Zugriff auf Admin-Portal

Wenn beim Zugriff auf das Admin-Portal eine Fehlerseite mit dem Hinweis angezeigt wird, dass ein bestimmter xml-Tag in der Datei „Web.config“ fehlt, entfernen Sie den Tag in der obersten Ebene des virtuellen Verzeichnisses des Portals aus der Datei „Web.config“ (kann über die IIS-Managementkonsole geöffnet werden).

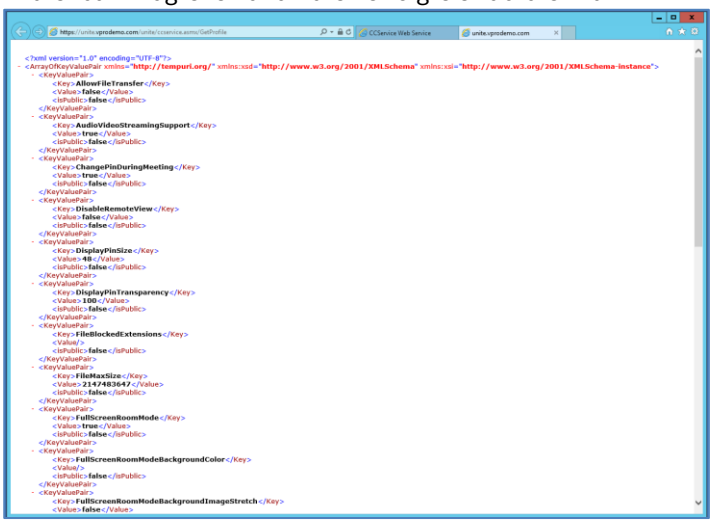
- Überprüfen Sie, ob die Installation des Webdienstes erfolgreich war, indem Sie auf den folgenden Link klicken:

    https://<yourservername>/unite/ccservice.asmx

    - Wählen Sie **GetProfile** aus.
    - Geben Sie **Test** in das **Wertfeld** ein und klicken Sie auf „Aufrufen“.



- Überprüfen Sie, ob Sie in der xml-Datei ein Standardprofil, wie unten dargestellt, anzeigen können. Dies ist ein Hinweis darauf, dass der PIN-Dienst auf die Datenbank zugreifen und Daten erfolgreich abrufen kann.



12.3 Fehler beim Starten der Hub Anwendung

Ein Pop-up-Fenster zeigt die Fehler-ID an. Basierend auf der ID kann die Art des Fehlers ermittelt werden.

12.3.1 Plattform-Prüfung fehlgeschlagen mit Fehler ID333333

Dieser Fehler zeigt an, dass der Hub eine Plattform-Prüfung bestanden hat, aber das Code Signing Zertifikat nicht validiert werden konnte. Dies liegt in der Regel an einem Betriebssystem, das kein aktualisiertes Stammzertifikat hat, wodurch das öffentliche Intel Unite Code Signing Zertifikat nicht validiert werden kann. Stellen Sie sicher, dass das System mit dem Internet verbunden ist, öffnen Sie einen Browser und navigieren Sie zu https://www.microsoft.com (Dies zwingt das System, die Stammzertifikate zu aktualisieren).

12.3.2 Plattform-Prüfung fehlgeschlagen mit Fehler ID666666

Dieser Fehler zeigt an, dass die Plattform nicht mit der Intel Unite Anwendung kompatibel ist. Wenden Sie sich an den OEM-Hersteller, um sicherzustellen, dass Sie eine unterstützte Plattform haben, um die Anwendung auszuführen.

12.4 Hub erhält vom PIN-Server keine PIN – es werden Strichlinien angezeigt.

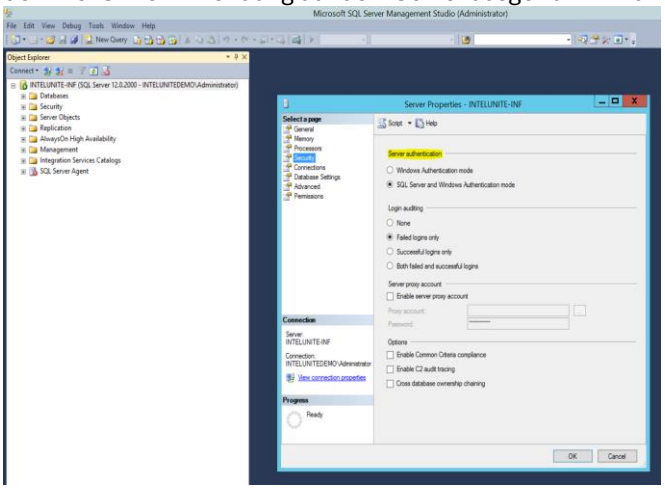
Starten Sie die Intel Unite Anwendung auf dem Hub mit einem Debug-Parameter, z. B. navigieren Sie von der Befehlsaufforderung zum Ordner, in dem die Anwendung gespeichert ist und führen Sie folgende Datei aus: **IntelUnite.exe** /debug
Dadurch öffnet sich ein Debug-Fenster und es werden die Verbindungsinformationen angezeigt. Unten sehen Sie eine Liste mit den häufigsten Fehlern und wie sie umgangen werden können. Wenn die Debug-Information einen dieser Fehler anzeigt, befolgen Sie die Lösungs-/Umgehungsschritte und beantragen Sie eine PIN auf dem Hub.

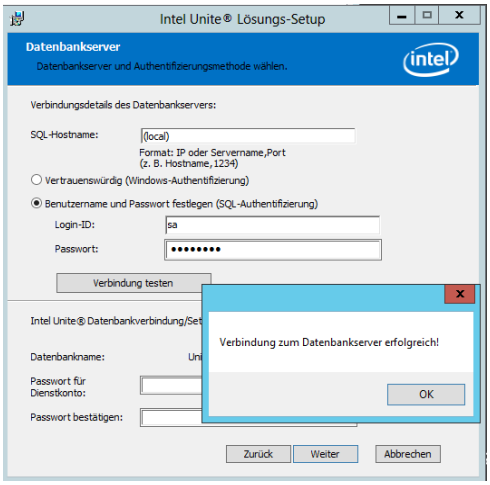
12.4.1 Server kann Anfrage nicht bearbeiten; Anmeldung des Benutzers „UniteServiceUser“ fehlgeschlagen.

Dieser Vorfall kann eintreten, wenn es bei der SQL-Anmeldung zu einer Abweichung kommt, oder wenn das Kennwort der Datenbank beschädigt wurde, da ein Benutzer versucht, Enterprise-Server mehrmals zu installieren.

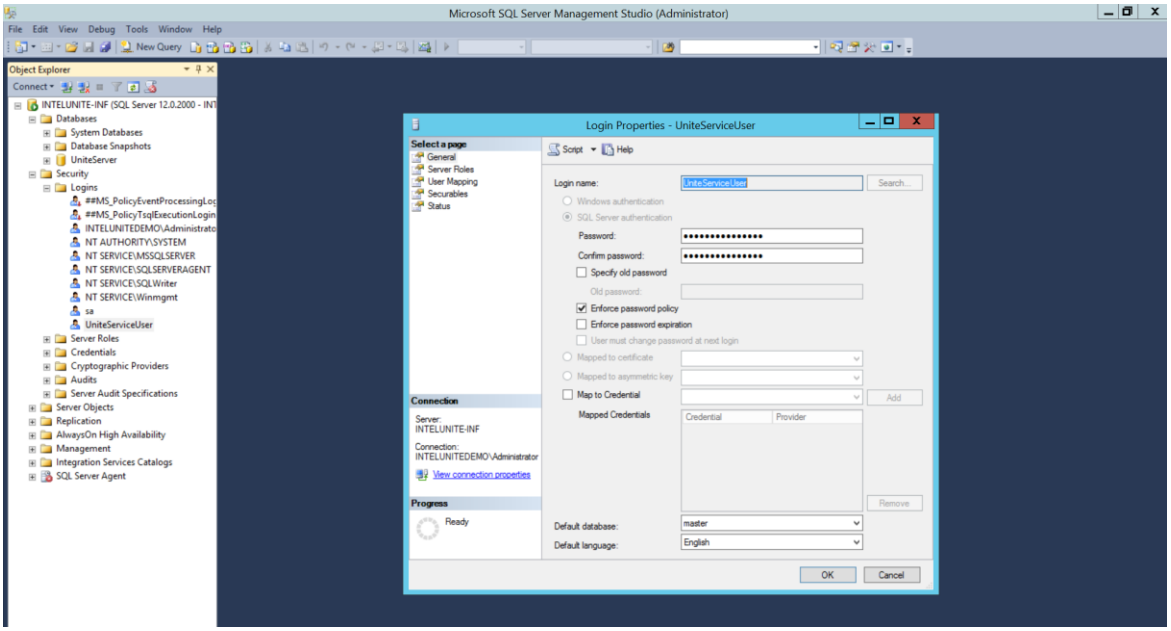
Umgehung/Lösung:

Überprüfen Sie die Authentifizierungs-Modi, die bei der MS-SQL-Installation verwendet werden. Zur Änderung des Anmelde-/Authentifizierungstyps gehen Sie zu Microsoft SQL Management Studio und verbinden Sie sich mit dem SQL-Server. Klicken Sie dann mit der rechten Maustaste auf den SQL-Server und wählen Sie „Eigenschaften“ aus. Wählen Sie die Seite „Sicherheit“ aus und überprüfen Sie, ob der Modus **SQL-Server und Windows-Authentifizierung** ausgewählt ist, wenn SQL-Authentifizierung beim Installieren der Intel Unite Anwendung auf dem Server ausgewählt wird.





Wenn der Fehler immer noch angezeigt wird, setzen Sie das Kennwort für **UniteServiceUser** zurück. Verbinden Sie sich über Microsoft SQL Management Studio mit Ihrem SQL-Server, gehen Sie zu **Sicherheit** > **Anmeldungen** und klicken Sie mit der rechten Maustaste auf **UniteServiceUser** um das Fenster **Anmeldungseigenschaften** zu öffnen. Geben Sie ein neues Kennwort ein und klicken Sie auf **OK**, um die Änderungen zu speichern.



12.4.2 Es werden keine Server aufgelistet. DNS-Diensteintrag _uniteservice._tcp wird versucht.

Umgehung/Lösung:

Dieser Fall kann eintreten, wenn der Hub den DNS-Eintrag nicht findet. Als Debug-Schritt öffnen Sie das Befehlszeilenfenster und führen Sie den Befehl nslookup aus. Vergewissern Sie sich, dass der Hub den Server, auf dem der DNS-Dienst ausgeführt wird, pingen kann und ein DNS-Eintrag für die Intel Unite-Lösung erstellt wurde. Der Diensteintrag muss folgende Werte aufweisen: **Dienst**: _uniteservice, **Protokoll**: _tcp, **Portnummer**: 443 und **Host, der den Dienst anbietet**: FQDN des Enterprise-Servers.

12.4.3 Vertrauenswürdige Verbindung für sicheren Kanal (SSL/TLS) konnte mit Autorität „uniteserverfqdn“ nicht hergestellt werden.

Die neueste Version der Intel Unite Lösung akzeptiert nur SHA-2-Zertifikate oder höher. Sie sollten mit Ihrer IT-Abteilung zusammenarbeiten, um sicherzustellen, dass das ausgestellte vertrauenswürdige Webserverzertifikat ein SHA-2-Zertifikat ist und der Zertifizierungspfad gültig ist.
Für eine Testumgebung können Sie ein SHA-2-Zertifikat erwerben oder die Verschlüsselung in Ihrer Umgebung deaktivieren.

- Um Unite ohne Verschlüsselung zu verwenden, überspringen Sie die nächsten Schritte, die Details über Site Bindings für den sicheren Port 443 bieten, und fahren Sie mit der Installation des MS SQL Servers und der Vorbereitung des DNS-Diensteintrags fort. Sie müssen auch sicherstellen, dass der Service auf Port 80 zu finden ist, wenn ein DNS-Diensteintrag erstellt wird.
- Ein anderer Weg zum Überspringen der Zertifikatsprüfung ist es, die Registrierung im Computerkonto des Hubs und Clients hinzuzufügen.
  HKEY_LOCAL_MACHINE\software\Intel\Unite\AllowInsecureCertificates (DWORD) [1 wenn die Algorithmusprüfung des Zertifikats übersprungen werden sollte, ansonsten 0. (wenn der Wert 0 ist, zwingen wir das Enterprise Zertifikat, ein SHA2-Zertifikat zu verwenden)]

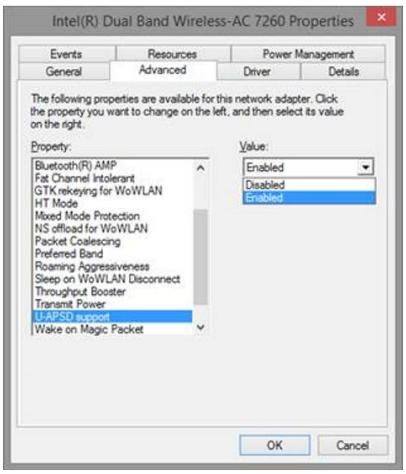
12.5 Client-Anwendung stürzt beim Starten/Verbinden ab

Führen Sie die Client-Anwendung mit einem Debug-Schalter aus und speichern Sie die Informationen in einer Protokolldatei.
(Führen Sie Intel Unite.exe /debug >logfile.txt aus)
Wenn die Protokolldatei die Meldung „AUSNAHME: -Schlüssel ist im angegebenen Status nicht gültig.“ enthält, schließen Sie die Anwendung und löschen Sie die Datei C:\Users\eaviles\AppData\Roaming\Microsoft\Crypto\RSA\[sid]\d046df.

12.6 Vorsicht: Es können Verbindungszeiten entstehen, die länger als üblich sind. Außerdem werden u. U. regelmäßige, langsam ablaufende Bildschirmaktualisierungen ausgeführt.

Ursache:

Hierbei handelt es sich um einen Fehler bei mehreren drahtlosen Zugriffspunkten, wenn U-APSD (Unscheduled Automatic Power Save Delivery) aktiviert ist. Siehe http://www.intel.de/content/www/de/de/support/network-and-i-o/wireless-networking/000005615.html.
Umgehung: Dieses Problem kann möglicherweise durch eine Aktualisierung der Firmware des drahtlosen Zugriffspunkts behoben werden. In den meisten Unternehmen ist dies jedoch keine einfache Aufgabe; ein letzter Ausweg kann die Deaktivierung von U-ASPD auf dem Client in den erweiterten Eigenschaften des Drahtlostreibers sein.



12.7 Vorsicht: Verlangsamung auf dem PIN-Server

Umgehung/Lösung: Der Enterprise-Server verwaltet das Zuweisen von PINs und sucht nach PINs, um sich mit Räumen verbinden zu können. Aus Sicherheitsgründen ist die Frequenz, mit der ein Benutzer PINs anfordern und aus der Datenbank PINs abrufen kann durch einen exponentiellen Backoff-Algorithmus beschränkt. Durch diesen Backoff-Mechanismus werden Versuche verzeichnet, die auf der IP-Adresse des Benutzers sowie seiner Anzahl an Versuchen basieren.

Produktionsserver können Lastenausgleichsmodule einsetzen, um die Auslastung zu steuern und die Redundanz in der Umgebung aufrechtzuerhalten. Lastenausgleichsmodule leiten den Datenverkehr zu den entsprechenden Web-Servern um. Dadurch scheint der Web-Server alle Anfragen von derselben IP-Adresse zu bekommen und der Backoff-Algorithmus wird ausgelöst.

Die Datenbank enthält eine gespeicherte Prozedur (*spGetPinBackoffTime*), über die die berechnete Verzögerung innerhalb von Sekunden an den Web-Server zurückgegeben wird. Diese Funktion kann deaktiviert werden, sodass die gespeicherte Prozedur immer 0 zurück gibt. Dadurch wird der Sicherheits-Backoff-Algorithmus deaktiviert.

12.8 Fehlerbehebung für Mac-Client:

Starten Sie die Intel Unite Anwendung (/Anwendungen/Dienstprogramme) über das Terminal, um die Debug-Benachrichtigungen anzuzeigen.
/pathToUnite/Intel\ Unite.app/Contents/MacOS/Intel\ Unite
Die Anwendung wird geöffnet und alle Debug-Informationen werden Ihnen im Terminal angezeigt.

12.8.1 Enterprise-Server, Verbindungsfehler 1003: Ein Server mit dem angegebenen Hostnamen konnte nicht gefunden werden.

Umgehung/Lösung: Überprüfen Sie, ob die DNS-Suchdomain korrekt definiert wurde.
Wenn ein Benutzer einen DNS-Server definiert, aber keine Suchdomains festlegt, steht dem MAC kein DNS-Domainsuffix zur Suche zur Verfügung, wenn er versucht eine Auto Discovery durchzuführen. Wenn keine DNS-Suchdomains definiert wurden, kann die Intel Unite Anwendung auch keine Domains zur Auto Discovery hinzufügen oder einen „statischen" Eintrag für *uniteservice* vornehmen. Erst dann, wenn Auto Discovery auf *_uniteservice._tcp* funktioniert, kann der Client den Enterprise-Server finden.
Die einfachste Lösung ist das Hinzufügen der DNS-Suchdomain (die mit dem DNS-SRV-Eintrag übereinstimmen sollte). Stattdessen kann auch der Enterprise-Server in den *plist*-Einstellungen definiert werden.
Verwenden Sie den Terminal-Befehl:
defaults write com.intel.Intel-Unite EnterpriseServer myServer.mydomain.myTLD

12.8.2 Enterprise-Server, Verbindungsfehler 1001: Anforderungszeitüberschreitung

Umgehung/Lösung: Dieser Fehler kann aus folgenden zwei Gründen auftreten:

1. Möglicherweise gibt es ein Problem mit dem Webdienst des Enterprise-Servers.
2. Mac hat ein Netzwerkproblem und kann sich nicht mit dem Server verbinden.

Zur Lösung des Problems muss zunächst der Webdienst im Debug-Protokoll gefunden werden. Suchen Sie nach https://yourserver/Unite/CCService.asmx.
Kopieren Sie diese URL und fügen Sie sie in Safari ein; überprüfen Sie, ob Ihr Mac auf den Webdienst zugreifen kann. Dadurch können Sie verifizieren, ob ein Netzwerkproblem bei der Verbindung zum Server besteht und ob der Webdienst auf dem Enterprise-Server ausgeführt wird.

12.8.3 Enterprise-Server Verbindungsfehler -1200: Ein SSL-Fehler ist aufgetreten und eine sichere Verbindung zum Server kann nicht hergestellt werden.

Arbeiten Sie mit Ihrer IT-Abteilung zusammen, um gültige SHA-2-Zertifikate zu erhalten, die für die Intel Unite Lösung benötigt werden.

12.9 Die Mac OS Intel Unite App wurde vom Client-Gerät entfernt/ deinstalliert und eine andere oder neuere Version der Intel Unite Anwendung wurde installiert, die alten Installationseigenschaften sind jedoch noch vorhanden.

Die Intel Unite Anwendung für Mac Client-Geräte folgt den allgemeinen OS X-Konventionen, daher werden Benutzereinstellungen nicht entfernt, wenn die App gelöscht wird.

Umgehung/Lösung:
Deinstallieren Sie die Intel Unite Anwendung auf dem Client-Gerät. Es gibt zwei Möglichkeiten, die Einstellungen zu entfernen und zu einem sauberen Status zurückzukehren.

1. Geben Sie im Terminal (/Anwendungen/Dienstprogramme) den folgenden Befehl ein:

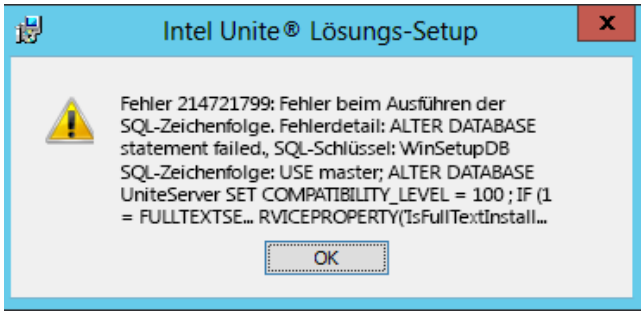
   defaults delete com.intel.Intel-Unite

2. Löschen Sie im Finder die Datei ~/Library/Preferences/com.intel.Intel-Unite.plist dann...

   Führen Sie einen Neustart des Systems durch. Plist-Dateien werden vom BS umfassend zwischengespeichert, deshalb können sie im Allgemeinen nicht gelöscht werden und das BS kann die Veränderung nicht annehmen.

12.10 Fehler 2147217900: Fehler beim Ausführen der SQL-Zeichenfolge.

Dieser Fehler wird generiert, wenn die Intel Unite-Serverinstallationsdatei und die Unite-Datenbank bereits vorhanden, aber der Servername leer ist.



Umgehung/Lösung:
Das Installationsprogramm löst eine Fehlermeldung aus, wenn die Datenbank bereits im Cluster existiert. Zum Beheben dieses Fehlers löschen Sie die Datenbank, vergewissern Sie sich, dass Sie über DBAdmin-Rechte verfügen und führen Sie das Installationsprogramm erneut aus.

12.11 Fehlermeldung: „Datenbankfehler“

Wenn ein IT-Administrator die Schaltfläche „Token senden“ aus der Admin-Konsole wählt und die Fehlermeldung „Datenbankfehler“ erhält, ist es wahrscheinlich, dass die SMTP-Servereinstellungen falsch sind. Sie müssen die SMTP-e-Servereinstellungen überprüfen.

12.12 Das Administrator-Webportal wird nicht richtig angezeigt (fehlende Komponenten)

Nach der Unite-Softwareaktualisierung wir das Administrator-Webportal nicht mehr vollständig angezeigt, es fehlen Komponenten wie Textfelder, Optionen oder Symbole. Die MIME-Typen werden durch die Option „Anforderungsfilter“ des IIS blockiert.

Umgehung/Lösung:

1. Öffnen Sie den IIS-Manager.
2. Rufen Sie die Eigenschaften für den IIS-Server auf.
3. Klicken Sie auf **MIME-Typen** und fügen Sie die JSON-Erweiterung hinzu:
    - Dateinamenserweiterung: .json
    - MIME-Typ: Anwendung/json
4. Gehen Sie zurück zu den IIS-Server-Eigenschaften.
5. Klicken Sie auf **Handler-Zuordnungen**.
    - Fügen Sie eine Skript-Karte hinzu
    - Fordern sie den Pfad „*.json“ an
    - Ausführbare Datei: C:\WINDOWS\system32\inetsrv\Asp.dll
    - Name: JSON
6. Gehen Sie im Bereich **Verbindungen** auf die Verbindung, Website, Anwendung oder das Verzeichnis, für die oder das Sie die Einstellungen des Anforderungsfilters ändern möchten.
7. Doppelklicken Sie im Bereich **Startseite** auf **Anforderungsfilterung**.
8. Suchen Sie „Dateinamenerweiterung zulassen“
9. Fügen Sie die folgenden 4 Erweiterungen hinzu:
    - .json
    - .less
    - .woff
    - .woff2

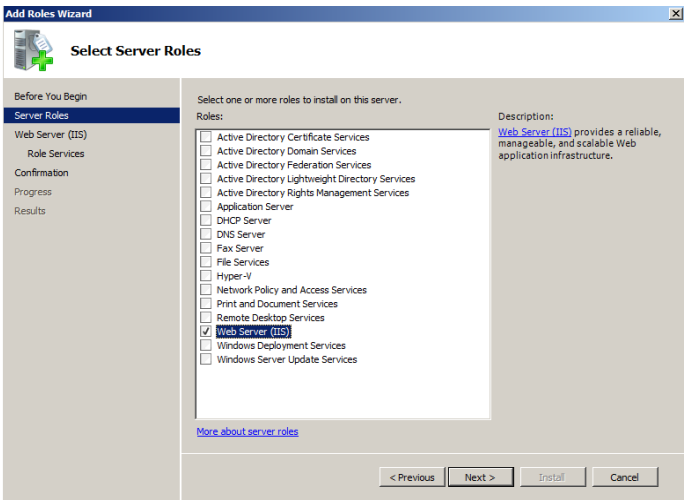
Anhang A: Enterprise-Server – Vorbereitung

Aktivieren von IIS

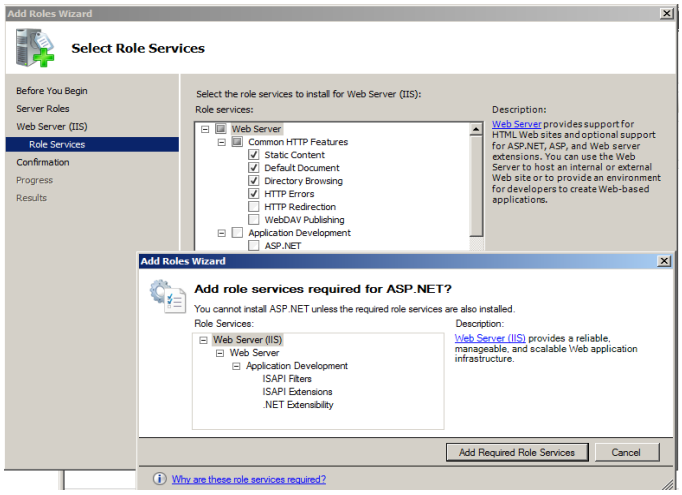
Für Windows 2008:

In Windows Server 2008 müssen Sie die Aktualisierung für .NET Framework 4.5 herunterladen (https://www.microsoft.com/en-us/download/details.aspx?id=40779)

- Klicken Sie auf **Start**, zeigen Sie auf **Administrative Tools (Verwaltung)** und klicken Sie auf **Server Manager**.
- Klicken Sie unter **Roles Summary (Rollenübersicht)** auf **Add Roles (Rollen hinzufügen)**.
- Verwenden Sie den **Add Roles Wizard(Assistent „Rollen hinzufügen“)** zum Hinzufügen der Rolle **Web Server (IIS)** (aktivieren Sie dieses Kästchen).



- Klicken Sie auf **Next (Weiter)**, bis das Fenster **Select Role Services (Rollendienste auswählen)** angezeigt wird.
- Überprüfen Sie, ob ASP.NET auch im Abschnitt **Application Development (Anwendungsentwicklung)** aktiviert ist. Wenn nicht, wählen Sie es aus. Bitte beachten Sie, dass ASP.NET nicht standardmäßig aktiviert ist. **Erforderliche Rollendienste zufügen** für ASP.NET. Sie benötigen auch ASP.NET 4.5.



- Gehen Sie nach dem Erstellen der Rolle im Menü **Roles (Rollen)** zu **Web Server (IIS)**. Öffnen Sie auf der rechten Seite des Fensters den **Internet Information Services (IIS) Manager (Internetinformationsdienste-Manager (IIS-Manager))** und wählen Sie den Server im linken Fenster unter **Connections (Verbindungen)** aus.

  Referenz: Link zur Windows Server-Bibliothek Installieren von IIS unter Windows Server 2008

  Hinweis: Die neueste Version der Intel Unite Lösung akzeptiert nur SHA-2-Zertifikate oder höher. Sie sollten mit Ihrer IT-Abteilung zusammenarbeiten, um sicherzustellen, dass das ausgestellte vertrauenswürdige Webserverzertifikat ein SHA-2-Zertifikat ist und der Zertifizierungspfad gültig ist.

  Für eine Testumgebung können Sie entweder mit Ihrem Certification Authority Team zusammenarbeiten, um ein SHA-2-Zertifikat zu erwerben, oder die Verschlüsselung deaktivieren.
  - Um Unite ohne Verschlüsselung zu verwenden, überspringen Sie die nächsten Schritte, die Details über Site Bindings für den sicheren Port 443 bieten, und fahren Sie mit der Installation des MS SQL Servers und der Vorbereitung des DNS-Diensteintrags fort. Sie müssen auch sicherstellen, dass der Service auf Port 80 zu finden ist, wenn ein DNS-Diensteintrag erstellt wird.
  - Alternativ können Sie die Zertifikatsprüfung überspringen, indem Sie den Registrierungsschlüssel im Computerkonto des Hubs und Clients hinzuzufügen. HKEY_LOCAL_MACHINE\software\Intel\Unite\AllowInsecureCertificates (DWORD) [1 wenn die Algorithmusprüfung des Zertifikats übersprungen werden sollte, ansonsten 0. (wenn der Wert 0 ist, zwingen wir das Enterprise Zertifikat, ein SHA2-Zertifikat zu verwenden)]

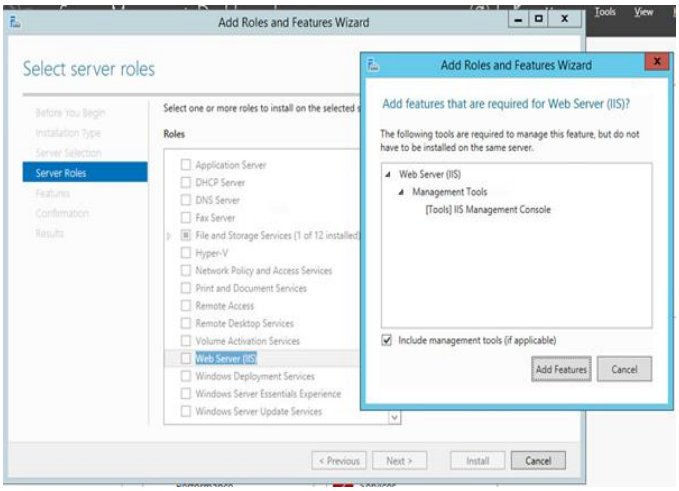
- Um ein Zertifikate zuzuweisen, erweitern Sie im Bereich **Verbindungen** (links) die Option „Sites“ und klicken auf **Standardwebsite**.
- Wählen Sie im rechten Fenster **Actions (Aktionen)** die Option **Bindings (Bindungen)** (unter „Site bearbeiten“) aus.
- Klicken Sie im Fenster **Site Bindings (Websitebindungen)** auf **Add (Hinzufügen)**.
- Verwenden Sie die folgenden Informationen:
  - Eingabe: https (Hinweis: nicht http)
  - IP Adresse: Alle nicht zugewiesen
  - Port: 443
  - Hostname: (leer lassen)
  - SSL Zertifikat: Verwenden Sie das SSL-Zertifikat, das in den vorherigen Schritten installiert wurde.

Klicken Sie auf **OK**.

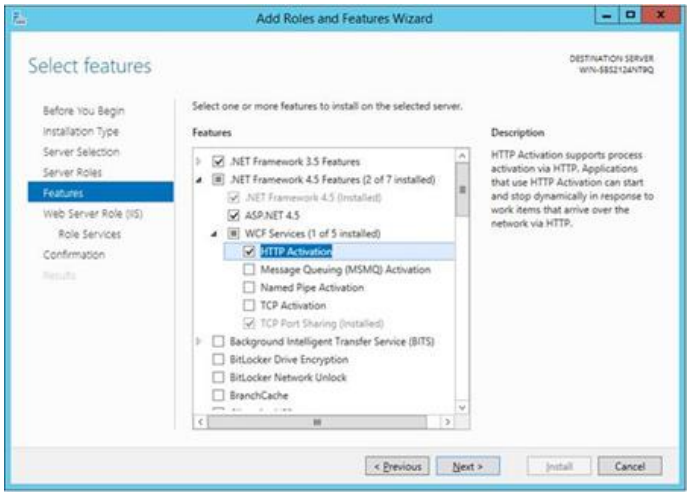
Windows 2012:

- Öffnen Sie den **Server-Manager**.
- Wählen Sie im Menü **Manage (Verwalten)** die Option **Add Roles and Features (Rollen und Funktionen hinzufügen)** aus.
- Wählen Sie **Role-based or Feature-based Installation (Rollenbasierte oder funktionsbasierte Installation)** aus.
- Wählen Sie den passenden Server aus (lokal ist standardmäßig aktiviert).
- Wählen Sie **Web Server (IIS)** aus und fügen Sie über **Add Features (Funktionen hinzufügen)** für den Webserver (IIS) erforderliche Funktionen hinzu. Klicken Sie auf **Next (Weiter)**.

HINWEIS: Falls Sie mehr Einzelheiten benötigen, um ein Internet Server Certificate im Unite Server anzufordern, gehen Sie zu folgendem Microsoft-Weblink https://technet.microsoft.com/en-us/library/cc732906.aspx und befolgen Sie die Schritte für SSL Zertifikat Anbieter, um ein signiertes Zertifikat zu erhalten.

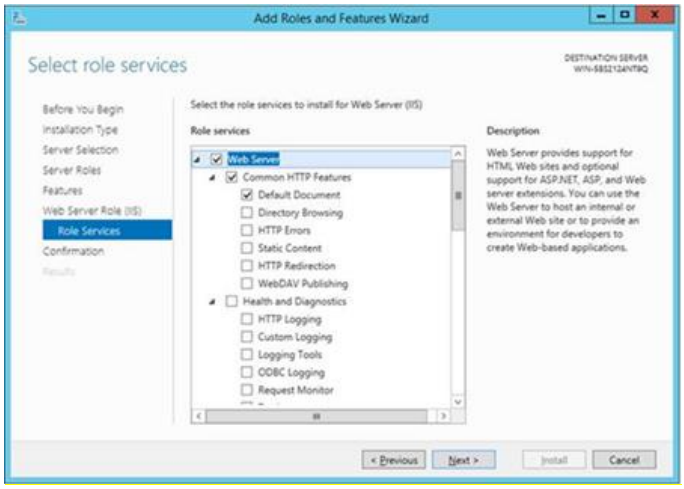


- Fügen Sie unter „Funktionen“ die folgenden Funktionen für IIS hinzu (da es sich hierbei nicht um Standardoptionen handelt):
  - .Net Framework 3.5-Funktionen
  - ASP.NET 4.5
  - WCF-Dienste
  - HTTP-Aktivierung (Fügen Sie bei Aufforderung für die HTTP-Aktivierung erforderliche Funktionen hinzu). Klicken Sie auf **Weiter**.



Hinweis: Eventuell wird von .NET 3.5 eine Fehlermeldung bei der Installation ausgegeben. Geben Sie einen alternativen Quellpfad an, wenn der Zielcomputer keinen Zugriff auf Windows Update hat. Klicken Sie auf den Link **Specify an alternate source path (Alternativen Quellpfad angeben)**, um den Pfad zum Ordner **\sources\sxs** auf den Installationsmedien anzugeben.
Referenz: https://technet.microsoft.com/en-us/library/dn482071.aspx

- Fügen Sie auf der Seite „Rollendienste“ **Web Server (IIS)** als Funktion zum Server hinzu oder akzeptieren Sie den Standardwert.
- Wählen Sie die folgenden Rollendienste aus, um den Webserver zu installieren:
    - Allgemeine HTTP-Funktionen
    - Standarddokument



- Klicken Sie auf **Next (Weiter)**, um fortzufahren und auf dem nächsten Fenster auf **Install (Installieren)**, um die ausgewählten Rollen und Funktionen zu installieren.
- Gehen Sie nach dem Erstellen der Rolle im Menü Rollen zu Web Server (IIS). Öffnen Sie auf der rechten Seite des Fensters den Internetinformationsdienste-Manager (IIS) und wählen Sie den Server im linken Fenster unter Verbindungen aus.

Hinweis: Die neueste Version der Intel Unite Lösung akzeptiert nur SHA-2-Zertifikate oder höher. Sie sollten mit Ihrer IT-Abteilung zusammenarbeiten, um sicherzustellen, dass das ausgestellte vertrauenswürdige Webserverzertifikat ein SHA-2-Zertifikat ist und der Zertifizierungspfad gültig ist.

Für eine Testumgebung deaktivieren Sie entweder die Verschlüsselung oder Sie erstellen ein eigensigniertes SHA 2-Zertifikat.

- Um Unite ohne Verschlüsselung zu verwenden, überspringen Sie die nächsten Schritte, die Details über Site Bindings für den sicheren Port 443 bieten, und fahren Sie mit der Installation des MS SQL Servers und der Vorbereitung des DNS-Diensteintrags fort. Sie müssen auch sicherstellen, dass der Service auf Port 80 zu finden ist, wenn ein DNS-Diensteintrag erstellt wird.
- Führen Sie den folgenden Powershell-Befehl als Administrator aus.
    - New-SelfSignedCertificate –dnsname "yourservername" –CertStoreLocation cert:\LocalMachine\My; wobei "yourservername" der FQDN des Enterprise-Servers ist.
- Alternativ können Sie die Zertifikatsprüfung überspringen, indem Sie den Registrierungsschlüssel im Computerkonto des Hubs und Clients hinzuzufügen. HKEY_LOCAL_MACHINE\software\Intel\Unite\AllowInsecureCertificates (DWORD) [1 wenn die Algorithmusprüfung des Zertifikats übersprungen werden sollte, ansonsten 0. (wenn der Wert 0 ist, zwingen wir das Enterprise Zertifikat, ein SHA2-Zertifikat zu verwenden)]

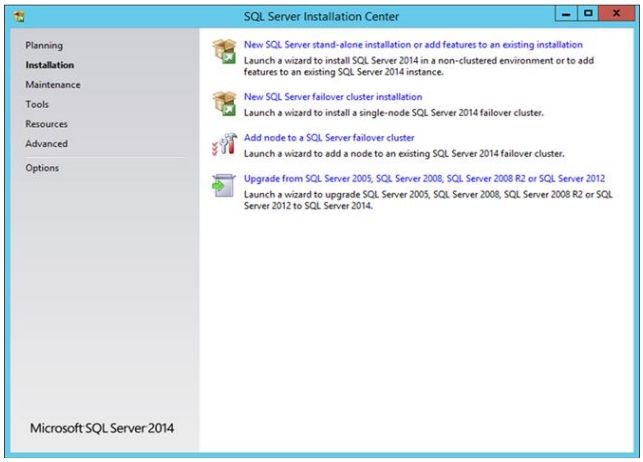
- Um ein Zertifikate zuzuweisen, erweitern Sie im Bereich **Verbindungen** (links) die Option „Sites" und klicken auf **Standardwebsite**.
- Wählen Sie im rechten Fenster **Actions (Aktionen)** die Option **Bindings (Bindungen)** (unter „Site bearbeiten") aus.
- Klicken Sie im Fenster **Site Bindings (Websitebindungen)** auf **Add (Hinzufügen)**.
- Verwenden Sie die folgenden Informationen:
    - Eingabe: https (Hinweis: nicht http)
    - IP Adresse: Alle nicht zugewiesen
    - Port: 443
    - Hostname: (leer lassen)
    - SSL-Zertifikat: (Wählen Sie das zuvor installierte Zertifikat aus.)
    - Klicken Sie auf **OK**.
- Klicken Sie auf **Close (Schließen)**.

Referenz: Link zu Windows Server-Bibliothek Installieren von IIS unter Windows Server 2012
Hinweis zu Port 443: Der Webdienst für die Intel Unit Anwendung kommuniziert über Port 443 mit den Clients und Hubs. Dieser Port muss wie oben beschrieben aktiviert sein.

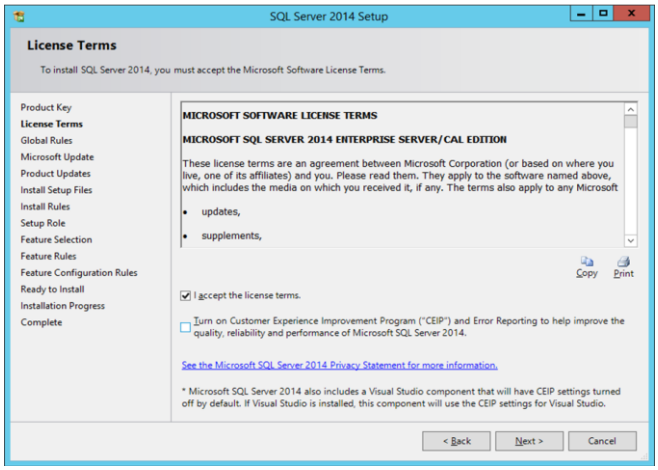
Microsoft SQL Server installieren

Für die Ausführung von Enterprise Server ist MS SQL erforderlich (Mindestvoraussetzung ist Version 2008 R2 oder höher). Sie können eine neuen, dedizierten SQL Server installieren, wenn Sie den Server in einer „Testumgebung“ laufen lassen möchten, um sich mit der Anwendung vertraut zu machen. Erforderlich ist dies jedoch nicht. Die Intel Unite Anwendung erstellt ohne Beeinträchtigung anderer Tabellen oder vorhandener Daten in der bestehenden Datenbank eine eigene Datenbank, Datentabellen und -indizes. Siehe unten für Installationsanweisungen für MS SQL 2014

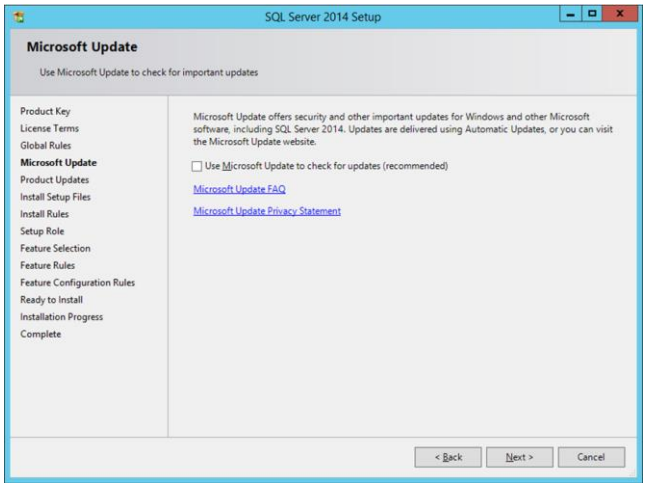
- Führen Sie das SQL Server-Setup aus und öffnen Sie das SQL Server-Installationscenter. Klicken Sie im linken Fenster auf **Installation** und wählen Sie **Neue SQL Server Standalone-Installation oder Hinzufügen von Funktionen zu einer vorhandenen Installation**.



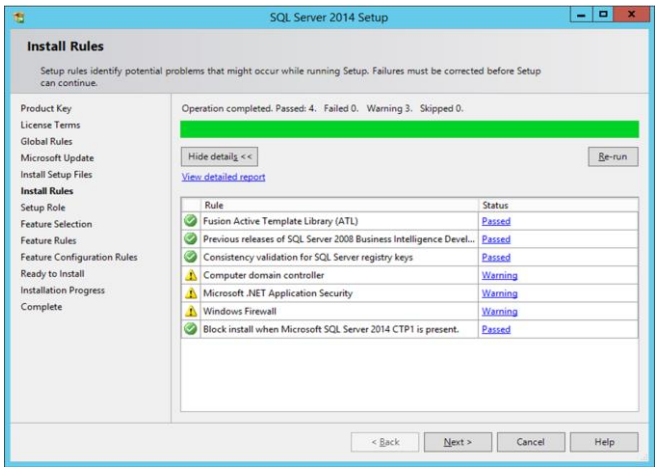
- Geben Sie den Product Key ein, stimmen Sie den Lizenzbedingungen zu und klicken Sie auf **Next (Weiter)**.



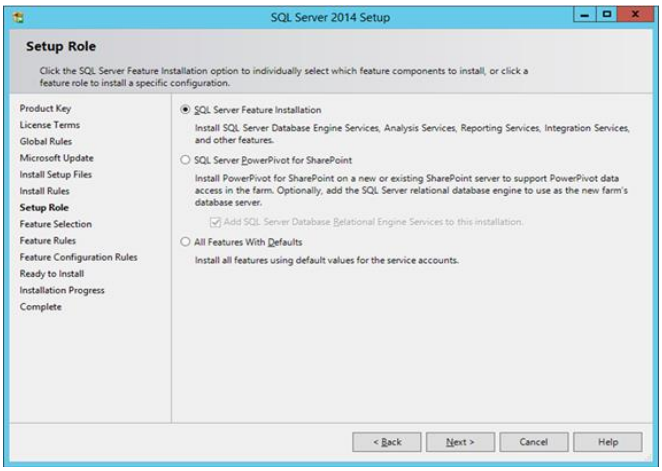
- Aktivieren Sie **Use Microsoft Update to check for updates (Microsoft Update zur Überprüfung auf Updates verwenden (empfohlen))**, um nach Updates zu suchen und klicken Sie auf **Next (Weiter)**. Auf der nächsten Seite sucht das Setup nach Produktaktualisierungen und installiert alle erforderlichen Aktualisierungen. Klicken Sie auf **Next (Weiter)**, um fortzufahren.



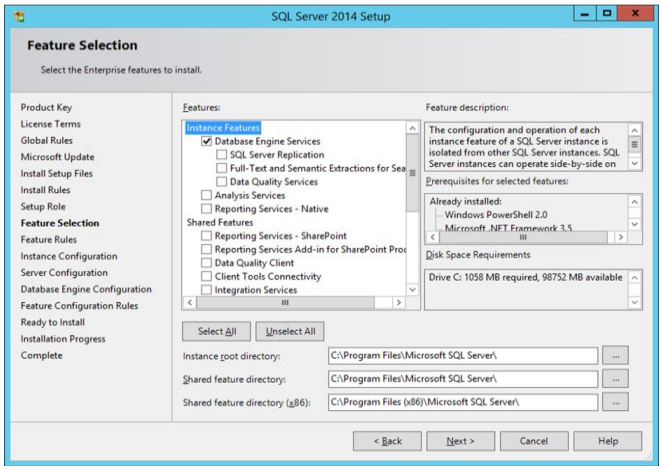
- SQL Setup sucht nach möglichen Fehlern und Anforderungen, die vor der Installation erfüllt werden müssen. Klicken Sie auf **Next (Weiter)**, um fortzufahren.



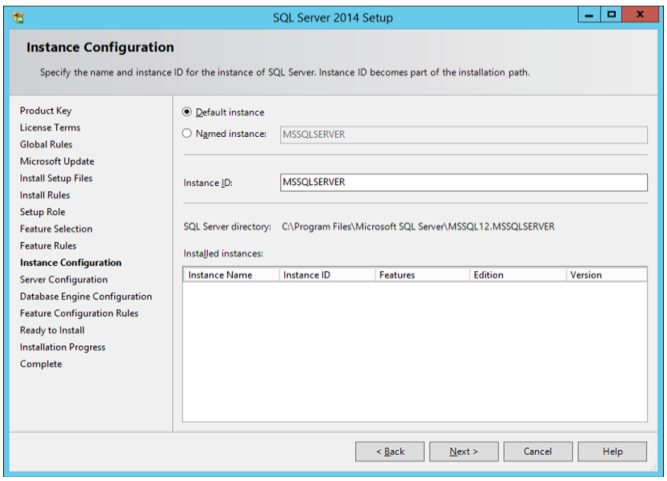
- Wählen Sie **SQL Server Feature Installation (SQL Server-Funktionsinstallation)** aus und klicken Sie auf **Next (Weiter)**.



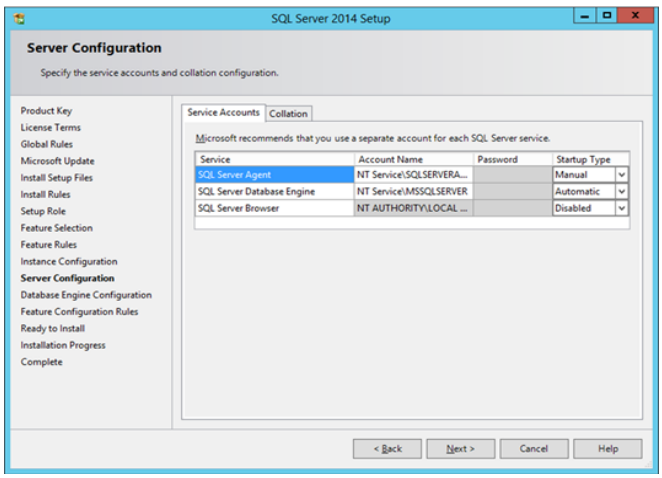
- Wählen Sie unter der **Feature Selection (Funktionsauswahl)** die Option **Database Engine Services (Datenbankmoduldienste)**, **Verwaltungstools– Abschließen** und klicken Sie auf **Next (Weiter)**.



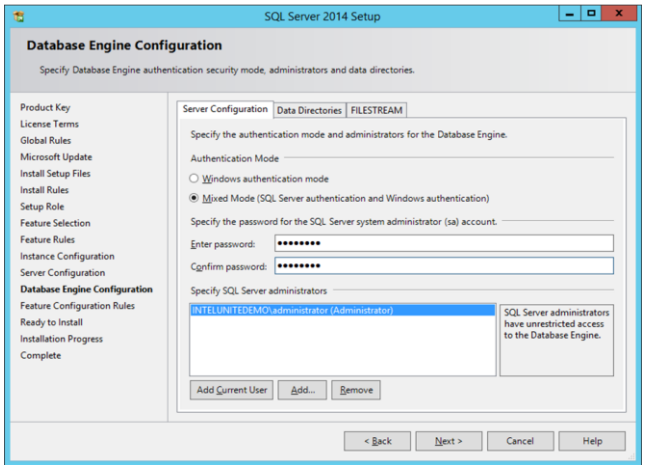
- Geben Sie den Namen und die Instanz-ID für den SQL Server an und klicken Sie auf **Next (Weiter)**.



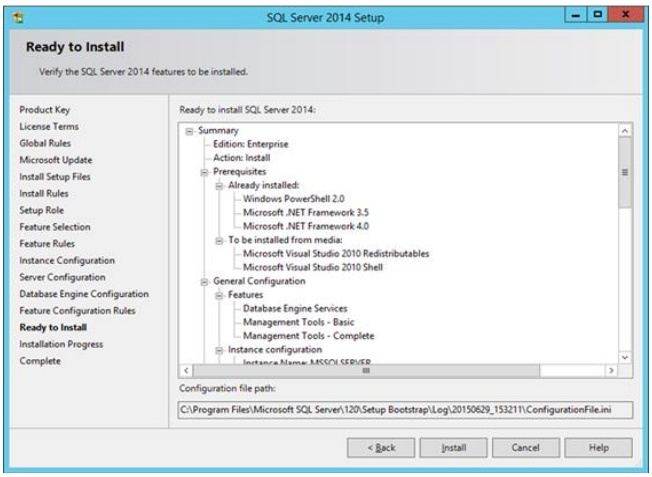
- Geben Sie die Dienstkonten für jeden Dienst an und klicken Sie auf **Next (Weiter)**, um fortzufahren.



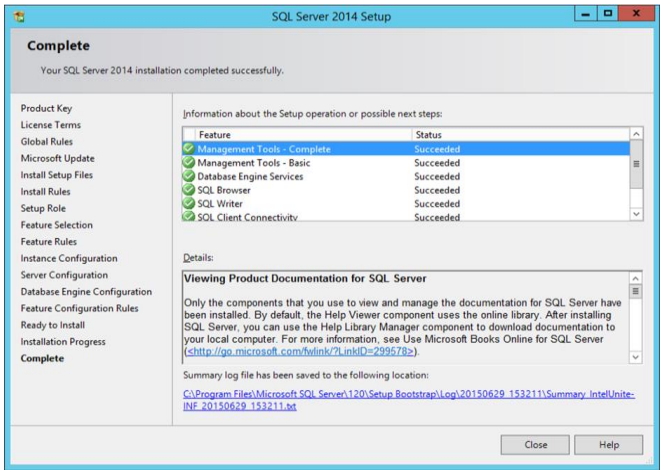
- Wählen Sie **Mixed Mode (Authentifizierung im gemischten Modus)** aus (dies schließt die Authentifizierung über den SQL Server und Windows ein), geben Sie die SQL Serveradministratoren an und klicken Sie auf **Next (Weiter)**.



- Überprüfen Sie die zu installierenden Funktionen und klicken Sie auf **Install (Installieren)**.



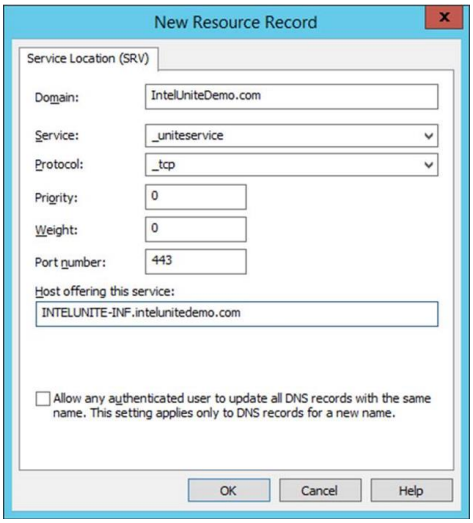
- **Schließen (Close)** Sie das Dialogfeld, wenn die Installation abgeschlossen ist.



Erstellen eines DNS-Diensteintrags

Der Hub und die Clients lokalisieren den Enterprise-Server über den DNS-Dienst in einer automatischen Suche nach dem Enterprise-Server. Sie können alternativ die manuelle Suche ausführen. Wir empfehlen jedoch dringend die Verwendung von DNS. Überspringen Sie diesen Abschnitt, wenn Sie den Enterprise-Server-Hostnamen manuell während der Hub- und Clientinstallation angeben wollen.
Bei Verwendung eines DNS-Diensteintrags sucht der Hub oder Client nach dem Dienst namens „_uniteservice._tcp“ in den folgenden DNS-Diensteinträgen:_uniteservice._tcp.example.com 86400 IN 0 5 443 uniteserver.example.com.
Einen DNS-Diensteintrag in Microsoft Windows hinzufügen:

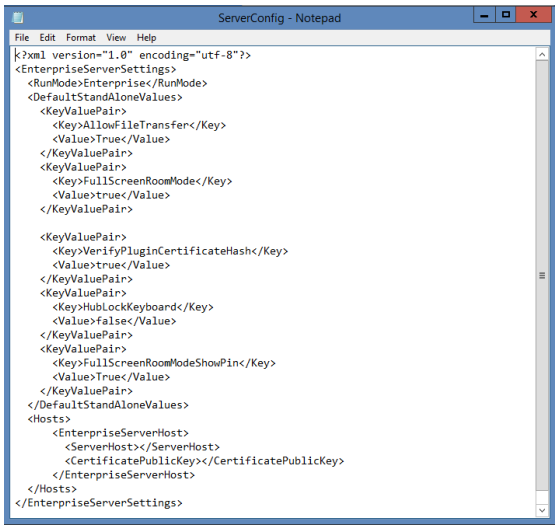
- Öffnen Sie im DNS-Server den DNS-Manager.
- Erweitern Sie die Forward-Lookupzonen (linker Bereich)
- Klicken Sie mit der rechten Maustaste auf die Zone und wählen Sie „Andere neue Datensätze…“ aus
    - Wählen Sie unter **Select a resource record type (Wählen Sie einen Ressourceneintragstyp:)** die Option **Service Location (SRV) (Dienstidentifizierung (SRV))** und anschließend **Create Record (Datensatz erstellen)** aus.
    - Geben Sie „_uniteservice“ bei **Service** ein.
    - Geben Sie „_tcp“ bei **Protocol (Protokoll)** ein.
    - Geben Sie „443“ bei **Port** ein.
    - Host, der diesen Service anbietet: Geben Sie Hostname/IP eines oder mehrerer Enterprise-Server ein.



HINWEIS: Gehen sie zu folgendem Microsoft-Link, dort finden Sie Einzelheiten zur Konfiguration eines DNS-Servers, der Weiterleitungen verwendet: https://technet.microsoft.com/en-us/library/cc754941.aspx

Anhang B Beispiel für ServerConfig.xml

Die Datei „ServerConfig.xml“ wird während der Installation von Hub- und Client-Komponenten der Intel Unite Software erstellt. Standardmäßig wird die xml-Datei (je nach Hub bzw. Client) an folgendem Ort abgespeichert: C:\Programmdateien (x86)\Intel\Intel Unite\Hub oder C:\Programmdateien (x86)\Intel\Intel Unite\Client
Diese Datei wird entsprechend bearbeitet, wenn Sie den **Server festlegen** und den Server-Hostnamen oder den **Public Key** manuell während der Installation von Intel Unite Software auf dem Hub oder Client eingeben.
Wenn Sie die Datei „serverconfig.xml“ nach der Installation konfigurieren möchten, navigieren Sie zu dem Ordner, in dem sich die Datei befindet, und nehmen Sie die nötigen Änderungen vor.



Wenn ein Server in der Datei „ServerConfig.xml“ definiert wurde, hat dieser Vorrang vor dem DNS-Diensteintrag.

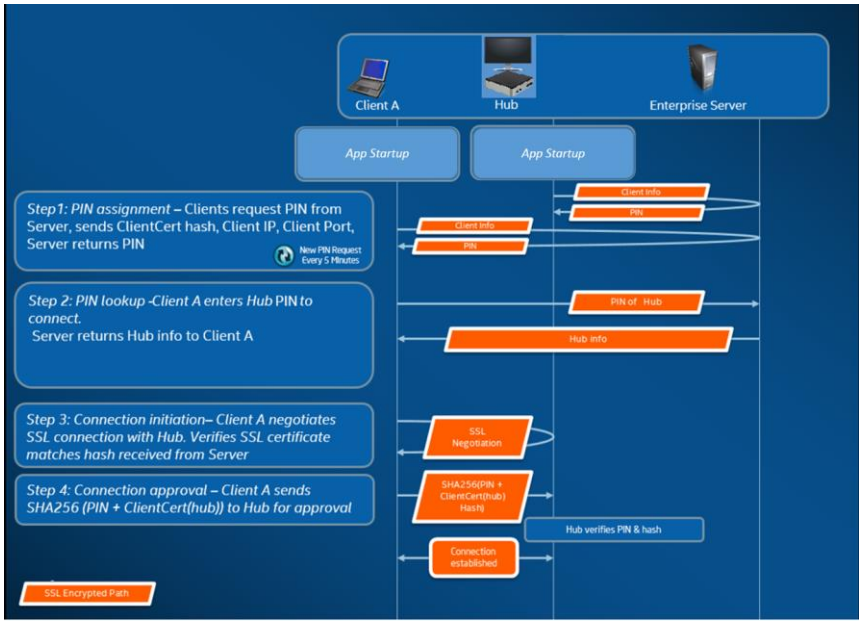
Anhang C Intel Unite Lösung – Übersicht über die Sicherheitsmerkmale

Intel Unite Software – Ablauf der Sicherheitsvorgänge

Dieser Abschnitt informiert Sie über die wichtigsten Sicherheitsaspekte der Intel Unite Anwendung. Es werden die Sicherheitsaspekte der folgenden vier Schritte erörtert:

1. PIN-Zuweisung
2. PIN-Suche
3. Initiierung der Verbindung
4. Genehmigung der Verbindung

In der folgenden Abbildung ist eine detaillierte Übersicht darüber zu sehen, wie die Anwendungen von Client (mit Intel vPro Technologie) und Hub auf sichere Weise PINs vom Enterprise-Server beziehen, PINs auflösen und eine Verbindung aufbauen.



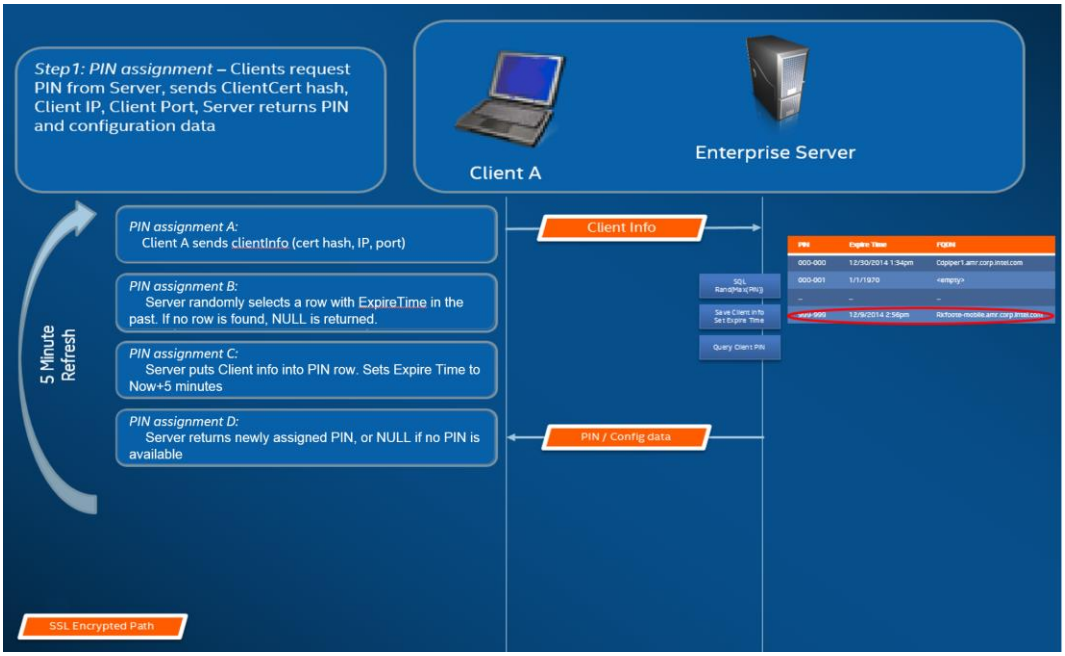
Schritt 1: PIN zuweisen

Die unten aufgeführte Abbildung zeigt, wie PINs zugewiesen werden. Die gesamte Netzwerkkommunikation während dieses Prozesses ist über einen Webdienst (TCP 443) SSL-verschlüsselt.
Der Hub und Client empfängt nicht nur PINs, sondern registriert auch die Verbindungsinformationen und einen öffentlichen Schlüssel am Server. Der öffentliche Schlüssel wird während der Verbindung genutzt, um zu überprüfen, ob jede Komponente mit dem beabsichtigten Ziel kommuniziert.

Hinweis: PIN-Zuweisung für Client (mit Intel vPro Technologie) und Hub folgen demselben Ablauf.

Beachten Sie auch Folgendes:

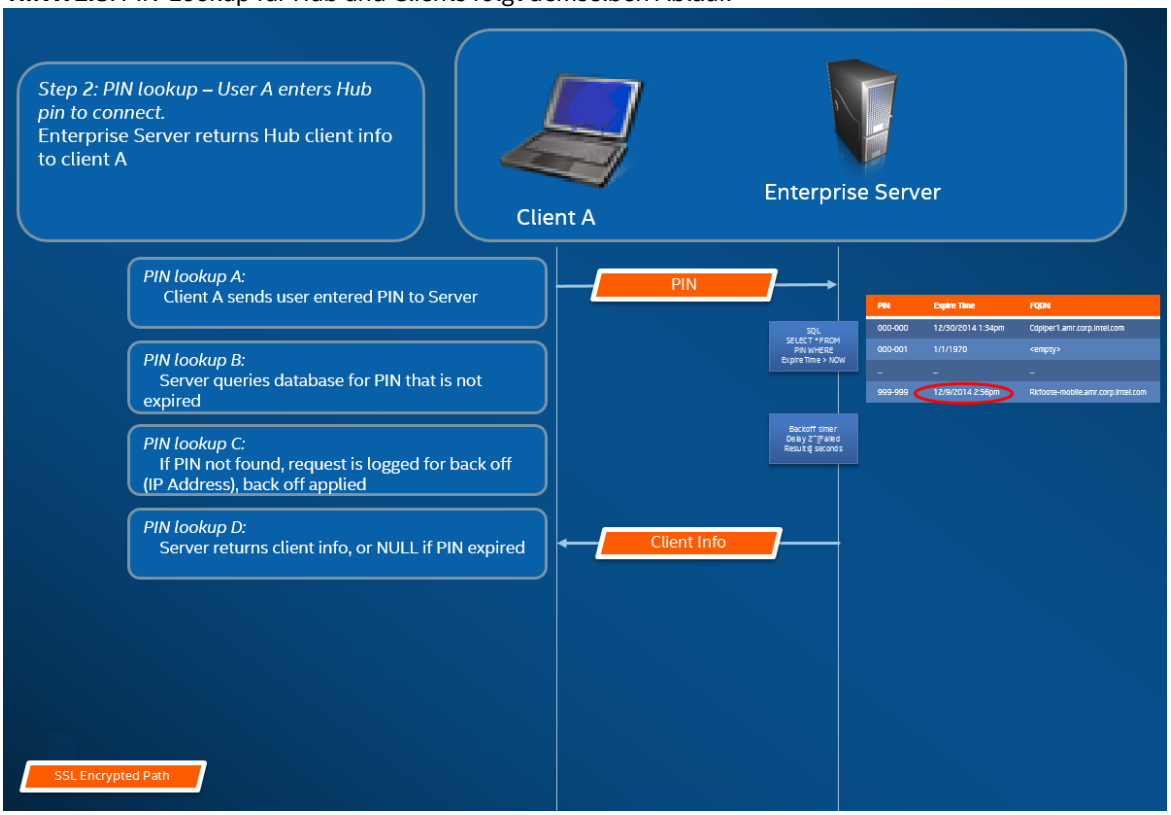
- Das PIN-Aktualisierungsintervall ist konfigurierbar.
- Wenn Hub oder Client Verbindungsinformationen senden, werden IP-Adressen im lokalen Host (127.0.0.0/8) und in den Bereichen 169.254.0.0/16 ignoriert.
- Der TCP-Port kann pro Client und Hub konfiguriert werden oder wird über ein Profil im Admin-Portal weitergegeben. Standardmäßig weist das Betriebssystem einen Port zu.
- Abgelaufenen PINs wird für bis zu 15 Sekunden Zugriff gewährt.
- Abgelaufene PINs werden bis zu 5 Sekunden nach Ablauf nicht neu zugeordnet, um zu vermeiden, dass sich ein Benutzer versehentlich mit dem falschen Display verbindet



Schritt 2: PIN-Lookup

Die unten aufgeführte Abbildung zeigt, wie PINs durch den Enterprise-Server aufgelöst werden. Die gesamte Netzwerkkommunikation während dieses Prozesses ist über einen Webdienst (TCP 443) SSL-verschlüsselt.
Wenn ein Benutzer eine Ziel-PIN im Intel Unite Client eingibt, sendet der Client die PIN an den Enterprise-Server, um sie als Verbindungsinformation aufzulösen. Nach einem erfolgreichen Lookup gibt der Enterprise-Server die gültigen Verbindungsinformationen des Ziels zurück. Bei dem Ziel kann es sich entweder um einen Hub oder einen Client handeln (mit Intel vPro Technologie), der die Intel Unite Software ausführt.
Dank des öffentlichen Schlüssels des Ziels können nicht nur Verbindungsinformationen empfangen werden, sondern kann die Client-Anwendung auch überprüfen, ob mit dem richtigen Ziel kommuniziert wird.

HINWEIS: PIN-Lookup für Hub und Clients folgt demselben Ablauf.

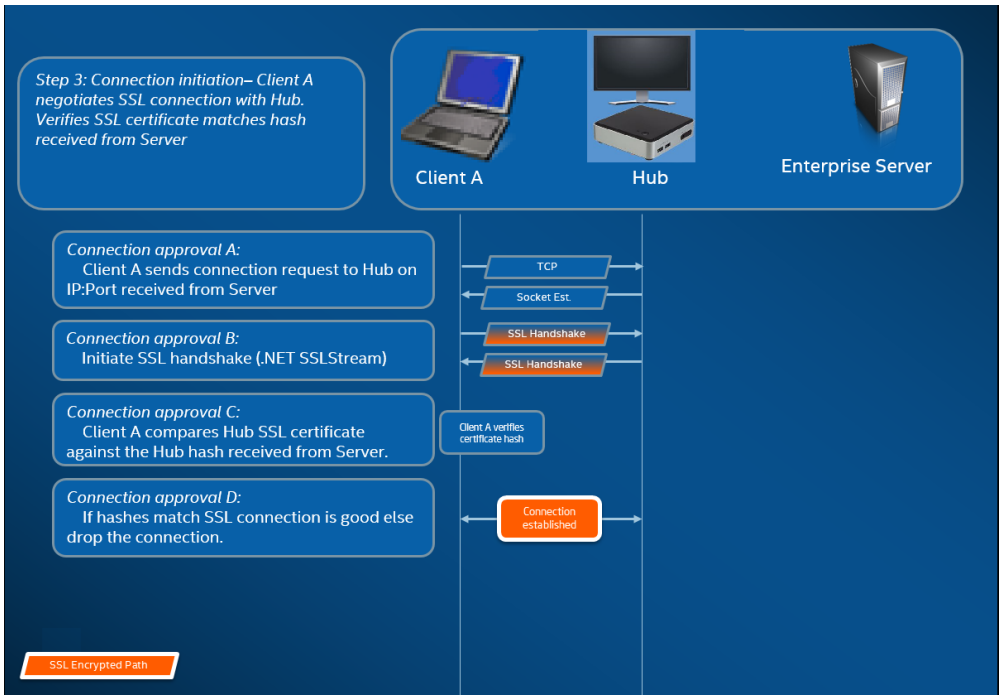


Backoff des PIN-Lookups

Um zu verhindern, dass Hacker PINs vom Enterprise-Server stehlen, werden fehlgeschlagene Versuche protokolliert. Ein Benutzer kann die PIN in 10 Sekunden bis zu 3-mal falsch eingeben, bis der Backoff-Mechanismus eine verzögerte Reaktion erzwingt (2^x Sekunden, wobei x=Anzahl der fehlgeschlagenen Versuche innerhalb von 5 Minuten).

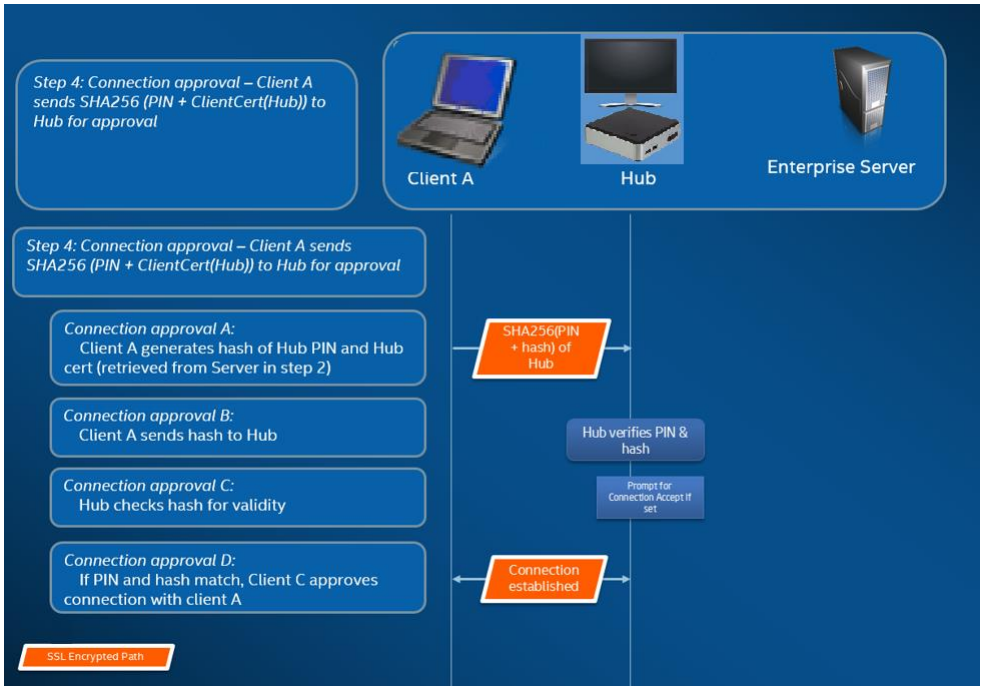
Schritt 3: Verbindung initiieren

Die unten aufgeführte Abbildung zeigt, wie eine Verbindung initiiert wird. Der Client initiiert eine TCP-Peer-to-Peer-Verbindung mit dem Ziel (ein Hub oder ein Client mit Intel vPro Technologie, der die Intel Unite Software ausführt) und startet einen SSL-Handshake. Das vom Ziel bereitgestellte Zertifikat wird „gehasht“ und mit dem Hash verglichen, das der Client in Schritt 2 empfangen hat. Mit diesem Vergleich werden Angriffe und Situationen, in denen IP-Adressen von DHCP-Clients wechseln, verhindert.



Schritt 4: Verbindung zulassen

Die unten aufgeführte Abbildung zeigt, wie die Verbindung zwischen dem Client und dem Ziel hergestellt wird. Bei dem Ziel kann es sich entweder um einen Hub oder einen Client handeln (mit Intel vPro Technologie), der die Intel Unite Software ausführt. Sobald das Ziel die PIN und das Client-Zertifikat verifiziert hat, wird die Verbindung angenommen und zwischen dem Client und dem Ziel hergestellt.



Anhang D Intel Unite Lösung – Lastenausgleichsmodul

Dieser Abschnitt beschreibt kurz, wie Sie das PIN-Backoff hinter dem Lastenausgleich/Proxy umgehen. Wenn Sie hinter einem Lastenausgleich stehen, wollen Sie sicher gehen, dass die SQL gespeicherte Prozedur dbo.spGetPinBackoffTime **immer 0 zurückgibt.**

Schritte:

- Ändern Sie die gespeicherte Prozedur dbo.spGetPinBackoffTime. Sie können alles auskommentieren und am Ende nur die „0 wählen“ verwenden.
- Führen Sie das Skript aus.

Wenn Sie nicht hinter einem Lastenausgleich stehen, wollen Sie sicher gehen, dass die SQL gespeicherte Prozedur den Standardwert behält.