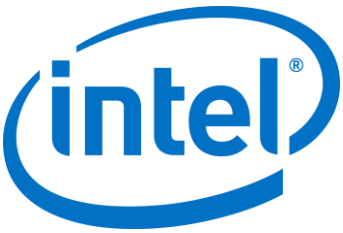
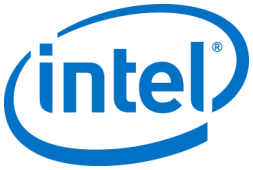


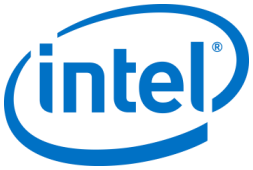
Solution Intel Unite®

Guide de déploiement en entreprise

Octobre 2017



Avertissements et copyright



Historique des révisions

Révision	Date Date	Remarques Notes
0.1	Nov 24, 2014	Outline
1.0	Apr 24, 2015	Review and Edit
1.1	May 7, 2015	Added Admin Web Portal
1.2	May, 12 2015	Product updates, name change
1.3	May 22, 2015	General updates to this guide
1.4	May 27, 2015	Update images
1.5	May 27, 2015	Update Profile Provisioning and Added Quiet Installers
1.6	Jun 5, 2015	Updates for new software released
1.7	Jun 8, 2015	Added more released features
1.8	Jun 9, 2015	Added Appendix, Architecture, additional overview details
1.9	Jun 16, 2015	Changed document flow and updates in deployment information
2.0	Jun 17, 2015	Added screenshots and IIS details
2.1	Jun 23, 2015	Added installation details and screenshots for Hub and Client
2.2	Jun 30, 2015	Added details on the installation process and on the uninstall instructions
2.3	Jul 7, 2015	Text fixes, added hyperlinks for easier navigation
2.4	Jul 21, 2015	Replaced image in section 2.1
2.5	Sep 7, 2015	Update Legal Disclaimers, removed NDA terms, removed Intel Confidential, added HKCU, additional formatting
2.6	Sep 10, 2015	Added new installers and new Quiet Installers
2.7	Oct 20, 2015	Added Appendix for Apple OSX
2.8	Dec 6, 2015	Added details on Enterprise Server installation for MS SQL installation and update images for version 2.0 app. Included Mac Client installation section under Client Installation and troubleshooting section.
2.9	Dec 16, 2015	Update images for consistency and re-arranged sections of installation instructions
3.0		Moved Mac out of the appendix, fixed TM&B and text. Moved Troubleshooting to the end, removed Appendix C
3.1	Jan 11, 2016	Update Admin portal section, changed footer, minor text changes
3.2	Jan 21, 2016	Trademark, text changes and layout fixes
3.3	Feb 25, 2016	Changed SQL min requirement from 2008 to 2008 R2
3.4	May 11, 2016	Update troubleshooting content for software version 3.0
3.5	May 25, 2016	Modified Enabling IIS section to include SHA-2 support, update Solution Requirements
3.6	May 31, 2016	Added registry keys and profile key-value pairs for 3.0
3.7	June 7, 2016	Added registry key to disable SHA-2 certificate, check for Windows under Enabling IIS section. Added additional clause on the Legal page, iPad Client install.

3.8	June 10, 2016	Added registry key, added a command for self-signed SHA 2 certificate for win server 2012, and registry keys for Guest Access
3.9	June 20, 2016	Re-arranged and fixed default values for the Profile keys table. Added Plugin Installation Notes and Certificate Hash Value section.
3.10	June 20, 2016	Update screenshots for v3.0
3.11	July 13, 2016	Added the *.dmg file for OS X install, fixed 5 default data types in Profile Configuration, added the "Supported SKU" in min requirements, plugin details and default colors in Profile Settings, added SKIP_EXTENDED_DISPLAY key
3.12	July 27, 2016	Added 12.8, text changes on section 5.6.1 and 5.6.2
3.13	Aug 21, 2016	Updates to section 5.6.1 and 5.6.2
3.14	Nov 16, 2016	Added Load Balancer, updated min req. for Win7. Added new Telemetry plugin and Reg Key ShowAvToggle. Changed order for plugin section. Added Microsoft web links. Changed default Profile window for the Admin Portal and A/V value to false.
3.1.1	Feb 17, 2017	Added New Features table, modified Server Req., added pics for Connect for Non-Window devices, substantial changes on the Admin Portal section 8, Intel Unite branding changes showed on pics, added 5 keys to Profile Configuration; moved logfile Reg Key from HKCU to HKLM. Added details on section 2.1, 4.2 and 8.7.3 for the SMTP email server. Changed Standalone to StandAlone. Removed 'repair' option from uninstall server.
3.1.2	Mar 5, 2017	Added new screenshots
3.1.3	Mar 17, 2017	Minor text changes, changed default login info for Admin Portal
3.1.4	Mar 31, 2017	Added deployment challenges for mobile devices on section 2.4 and 6.1, delete "tablet" from section 6.5
3.1.5	Apr 3, 2017	Added section 12.12 to Troubleshooting section (Admin Web Portal issue)
3.1.6	Apr 13, 2017	Update screenshots on section 6.5, 8.2, 8.4.2, 12.4.1. Modified default values for "Allow File Transfer, Audio Video Streaming Support" on table 8.7.1
3.1.7	May 3, 2017	Changed min requirements for the Server from 2012 to MS 2008 and Server SQL 2008 R2 (as documented on earlier guide versions)
3.2.1	Oct 18, 2017	Added a new Server installer image with the Host FQDN setting on section 4.3, a new column on the table in section 1.3, Whiteboard & Telemetry plugin details on section 5.6. Changed min iOS requirement on section 2.3. Fixed "Full Screen Room Mode" & "Full Screen Room Mode Show Pin" to True on section 8.7.1.
3.2.2	Oct 27, 2017	Added section 8.7.5 Setup for Moderators and a note for setup moderators on section 8.5.4 paragraph C.

Table des matières

1 Introduction

Le logiciel Intel Unite® permet la sécurisation et la connexion des salles de réunion, pour une collaboration simplifiée. Il a été conçu pour connecter facilement et rapidement tous les participants pendant une réunion. La solution Intel Unite® est une solution simple de collaboration instantanée qui répond à vos besoins actuels et constitue la base de fonctionnalités et d'innovation futures.
Ce document décrit comment installer le logiciel Intel Unite® en mode Entreprise et peut être utilisé pour en savoir plus sur les fonctionnalités de la solution et à des fins de dépannage.

1.1 Public visé

Ce document est destiné aux professionnels de l'informatique des entreprises et aux personnes chargées du déploiement de la solution Intel Unite® dans un environnement d'entreprise.

1.2 Terminologie et définitions de la solution Intel Unite®

Serveur d'entreprise (serveur) : ce terme désigne le serveur Web et le service PIN s'exécutant sur le serveur qui attribue et saisit les codes PIN. Il fournit une page de téléchargement pour les clients et le portail administrateur pour la configuration.

Client : ce terme désigne l'appareil (Windows*, macOS*, iOS*, Android* ou Chromebook*) utilisé pour se connecter au concentrateur.

Concentrateur : ce terme renvoie à l'ordinateur au format mini doté de la technologie Intel® vPro™ qui est connecté à l'écran dans une salle de conférence et qui exécute l'application Intel Unite®.

FQDN : cet acronyme signifie Fully Qualified Domain Name (nom de domaine complet de l'hôte).

Plugin : ce terme renvoie à un composant logiciel installé sur le concentrateur qui étend les fonctionnalités de la solution Intel Unite®.

IIS : cet acronyme signifie Internet Information Services, un serveur Web fournit par Microsoft*.

1.3 Nouveautés de la solution Intel Unite®

Afin de vous aider à repérer les éléments ajoutés au logiciel Intel Unite® du point de vue du déploiement, le tableau suivant récapitule les fonctions ajoutées au présent guide de déploiement.

Les nouvelles fonctionnalités pour les appareils clients sont répertoriées dans le Guide de l'utilisateur de la solution Intel Unite®.

v 2.0	v 3.0	v 3.0 MR	v 3.1	v 3.2
Affichage étendu	Streaming audio/vidéo pour Windows accéléré par le matériel (1080p à 20-30 ips)	Prise en charge de la présentation sous iOS	Expérience utilisateur améliorée sur le portail administrateur, environnement différent grâce, notamment, à l'ajout de boîtes de dialogue permettant une sélection plus simple des paramètres	Ajout d'un paramètre de portail administrateur au programme d'installation du serveur. Mise à jour de WebAPI Web.Config afin d'inclure l'URL du portail administrateur
Prise en charge de Windows 10	Plug-in d'accès invité en mode protégé		Portail administrateur : planification de réunions	Ajout du plug-in Whiteboard à la liste des plug-ins
Plug-in de connexion des utilisateurs invités	Réunions prévues (une seule pièce)		Portail administrateur : mode de modérateur	Nouvelle version minimale requise d'iOS : 10.1
Plug-in pour Skype Entreprise	Verrouillage de la réunion		Portail administrateur : code PIN statique	
	Prise en charge de l'affichage sous iOS		Portail administrateur : réservation du code PIN	
			Portail administrateur : transparence du code PIN	
			Portail administrateur : désactivation de l'affichage à distance	
			Prise en charge de Chrome OS	
			Prise en charge d'Android	

2 Configuration requise pour l'installation de la solution Intel Unite®

2.1 Configuration requise du serveur d'entreprise

- Microsoft Windows* Server 2008 ou version ultérieure
- Microsoft Internet Information Services avec chiffrement SSL
    - Cela implique de disposer d'un certificat de serveur Web SHA2 avec une racine de confiance interne ou publique.
- Serveur de messagerie SMTP configuré sous Microsoft Internet Information Services
- Microsoft SQL Server 2008 R2 ou version ultérieure
    - Dernier niveau des correctifs recommandé
- Microsoft .NET* 4.5 ou version supérieure
- 4 Go de RAM
- 32 Go de stockage disponible
  REMARQUE : le serveur Web IIS et la base de données Microsoft SQL peuvent être installés sur des machines différentes.

2.2 Configuration requise du concentrateur

- Microsoft Windows 7 SP1, 8.1 ou 10 (32 bits et 64 bits)
    - Dernier niveau des correctifs recommandé
- Microsoft .NET 4.5 ou version supérieure
- UGS[1] pris en charge : mini PC doté du processeur Intel® Core™ vPro™ de 4e génération ou plus récent
- Connexion réseau filaire ou sans fil
- 4 Go de RAM
- 32 Go de stockage disponible

2.3 Configuration requise du client

- Microsoft Windows 7 SP1, 8.1 ou 10 (32 bits et 64 bits)
    - Dernier niveau des correctifs recommandé
- Microsoft .NET 4.5 ou version supérieure
- OS X* 10.10.5 ou version supérieure
- iOS 10.1 ou version supérieure
- Connexion réseau filaire ou sans fil

[1] Communiquez avec votre fabricant ou un représentant Intel pour connaître les UGS pris en charge.

2.4 Considérations informatiques et conditions réseau

L'installation du concentrateur et du client doit s'effectuer selon les processus établis par votre service informatique en matière de distribution logicielle.
Pour une fiabilité assurée, il est vivement recommandé que le concentrateur utilise une connexion réseau filaire. Cela permet d'éviter la saturation de la bande passante, particulièrement dans les zones encombrées.
Veillez également à faire en sorte que le logiciel Intel Unite® accepte les connexions entrantes. Cela peut nécessiter l'ajout d'une exception au pare-feu installé sur le concentrateur. Contactez votre fournisseur de pare-feu pour obtenir des informations spécifiques sur la création d'exceptions d'application.

Dans un environnement de production, il est vivement conseillé d'utiliser un FQDN (Fully Qualified Domain Name) et de configurer un enregistrement de service DNS pointant vers le serveur d'entreprise. Il s'agit du moyen le plus simple pour permettre aux concentrateurs et aux clients de localiser le serveur d'entreprise.
Pour les mises à niveau de sécurité, l'application accepte uniquement les certificats SHA-2 ou supérieurs. Vous devrez peut-être mettre à niveau les certifications sur votre serveur Web. Communiquez avec l'équipe responsable de la sécurité informatique pour obtenir des certificats SHA-2 pendant la configuration.

2.4.1 Appareils clients mobiles

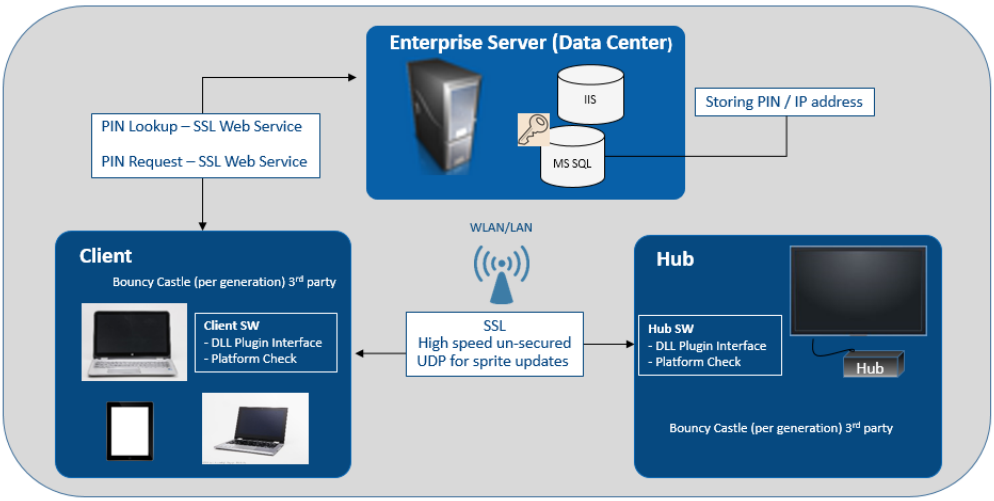
Si votre entreprise envisage de déployer des appareils clients mobiles sur le système d'exploitation du client Intel Unite®, prenez en compte ce qui suit :
Pour pouvoir se connecter à la solution Intel Unite®, tous les appareils clients (y compris les appareils iOS et Android) doivent être connectés au réseau d'entreprise ou utiliser un VPN configuré de manière adéquate. Il se peut que les tablettes et les téléphones normalement utilisés à des fins personnelles et qui ne sont pas connectés au réseau d'entreprise, mais au réseau de leur propre opérateur, ne puissent pas rejoindre une session de l'application Intel Unite® : il est possible en effet que vous disposiez d'un pare-feu d'entreprise qui empêche une telle connexion.

À l'attention des administrateurs informatiques :

- Si les utilisateurs de l'application Intel Unite® utilisent leurs propres appareils mobiles, assurez-vous qu'ils sont connectés au réseau d'entreprise afin qu'ils puissent rejoindre Intel Unite® ou faites en sorte de trouver un moyen d'autoriser les connexions de ces appareils à l'application.
- Vérifiez que vous disposez des outils nécessaires pour gérer convenablement ces appareils et assurer la sécurité du réseau.
- Mettez en place une stratégie adéquate pour gérer ces appareils qui peuvent poser un risque supplémentaire pour la sécurité.
- Mettez en place une politique de gestion des appareils mobiles relative aux appareils personnels ou aux appareils mobiles destinés à une utilisation professionnelle.
- La stratégie de sécurité en place devrait assurer la protection des données en fonction de leur confidentialité. Les niveaux de protection dépendent du niveau de criticité que votre entreprise accorde à ses données et des mesures que vous êtes prêt à mettre en place pour assurer leur sécurité.

3 Présentation du processus de déploiement

La solution Intel Unite® comporte trois composants : un serveur d'entreprise, un concentrateur et un client. Le serveur d'entreprise est le premier composant à configurer. Lors de leur démarrage, les applications du concentrateur et du client utiliseront le serveur d'entreprise pour échanger des informations de connexion et recevoir les codes PIN attribués.
Le concentrateur est le mini PC doté du processeur Intel® Core™ vPro, qui est généralement connecté à un affichage ou à un projecteur dans une salle de conférence.
Les clients suivent les instructions affichées sur le concentrateur pour télécharger le logiciel client et se connecter au concentrateur en saisissant le code PIN qui s'affiche. Une fois connecté, le client peut présenter du contenu, l'afficher et l'annoter, partager des fichiers avec d'autres participants connectés au même concentrateur et interagir grâce aux plug-ins installés sur le concentrateur.
Ce schéma fournit un aperçu des composants installés.



3.1 Ressources de déploiement

Pour terminer l'installation, vous devez disposer :

- des droits d'administration de la base de données
- des droits d'administration du serveur d'entreprise
- des droits d'administration du concentrateur

Vous pourrez également avoir besoin :

- que l'administrateur informatique de sécurité émette un certificat SHA-2
- des droits d'administration des stratégies de pare-feu
- des droits d'administration pour créer un enregistrement de service DNS, utilisé par le concentrateur et les clients pour localiser le serveur d'entreprise (vivement recommandé)

4 Installation du serveur d'entreprise

4.1 Présentation du serveur d'entreprise

Le programme d'installation du serveur d'entreprise inclut la base de données, le serveur PIN, le portail Web administrateur et la page de téléchargement du client.
Le serveur d'entreprise contient 4 composants :

1) La base de données Microsoft SQL conserve toutes les informations d'état de l'infrastructure de la solution Intel Unite®.
2) Le service Web est un service de messagerie normalisé qui communique avec la base de données, les concentrateurs et les clients.
3) Le site Web du portail administrateur gère les concentrateurs et les clients, génère des statistiques et fournit un service de surveillance et d'alerte.
4) La page de téléchargement de clients contient le logiciel Intel Unite® pour le client.

En outre, il est important de savoir que les concentrateurs et les clients localisent votre serveur d'entreprise sur votre infrastructure réseau selon les deux méthodes suivantes : fichier ServerConfig.xml ou enregistrement de service DNS.
Il est conseillé d'utiliser un enregistrement de service DNS, car cela permet la mise en place d'une configuration Zero Touch du client et du concentrateur. Consultez la rubrique relative à la Création d'un enregistrement de service DNS. Toutefois, si vous n'êtes pas en mesure d'acquérir un enregistrement de service DNS, il est possible de configurer le serveur d'entreprise dans le fichier ServerConfig.xml. Consultez l'annexe B pour obtenir un exemple de fichier ServerConfig.xml.

4.2 Pré-installation du serveur d'entreprise

- Vérifiez que le serveur satisfait bien à la configuration logicielle et matérielle minimale requise.
- Vérifiez qu'IIS version 8.0 ou version ultérieure est installé sur votre serveur. IIS doit être activé pour que l'installation via le programme d'installation du serveur aboutisse. Pour obtenir de l'aide quant à l'activation et la configuration d'IIS, consultez la rubrique Activation de IIS.
- Configurez le serveur de messagerie SMTP sous le Gestionnaire des services Internet (IIS). Voir la section
- Paramètres du serveur de messagerie électronique.
- Assurez-vous que vous avez bien installé et activé ASP.NET 4.5.
- Veillez à ce que le chiffrement SSL soit activé sur IIS (les sites https devraient fonctionner). **REMARQUE :** vous devrez peut-être faire appel à votre service informatique pour installer un certificat SHA-2 avec une racine de confiance valide.
- Assurez-vous que vous disposez des droits d'accès administrateurs à MS SQL à l'aide de l'authentification Windows ou SQL. Pour ce faire, consultez la rubrique Installation de Microsoft SQL Server.
- Ajoutez un enregistrement de service DNS pour lancer la recherche automatique du serveur d'entreprise. Consultez la rubrique relative à la Création d'un enregistrement de service DNS.

4.2.1 Mise à niveau logicielle

Si votre entreprise effectue une mise à niveau logicielle :

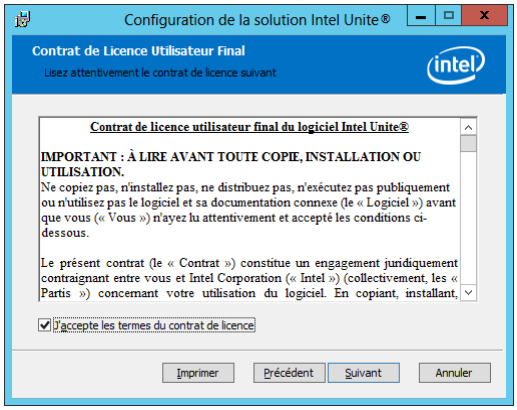
- Assurez-vous de sauvegarder votre base de données : en effet, les modifications ne peuvent pas être annulées.
- Toutes les connexions à la base de données doivent être fermées avant la mise à niveau (déconnectez-vous du portail administrateur).

- Lors de la mise à niveau, l'option Base de données est sélectionnée par défaut (aussi bien pour les installations locales qu'à distance) si le fichier 'Intel Unite serveur.msi' est exécuté sur le serveur PIN.

4.3 Installation du serveur d'entreprise

Une fois toutes les étapes de la section précédente (Pré-installation du serveur d'entreprise) vérifiées, poursuivez avec les programmes d'installation du logiciel Intel Unite® (ce processus doit être exécuté sur le serveur qui héberge l'environnement IIS).

- Localisez le fichier **Intel Unite Server.mui.msi** et double-cliquez pour l'installer sur le ou les serveurs cibles.
- L'assistant d'installation vous propose d'installer les composants suivants : base de données, service Web, page de téléchargement du client et portail administrateur.
- Après avoir lancé **Intel Unite Server.mui.msi**, acceptez le contrat de licence en cochant la case **J'accepte les termes du contrat de licence**.



- Cliquez sur **Suivant** pour passer à la fenêtre Serveur de base de données.
- Dans la fenêtre Serveur de base de données, sélectionnez **Informations de connexion au serveur de base de données**. Les options disponibles sont les suivantes :

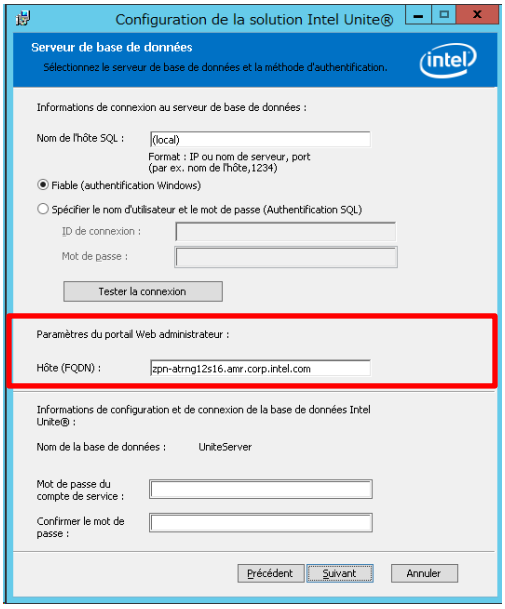
➢ Dans la boîte de dialogue **Nom de l'hôte SQL**, **(local)** est la valeur par défaut du serveur SQL. Vous pouvez la modifier en changeant le nom de l'hôte ou conserver la valeur par défaut (en laissant **(local)** si SQL est installé sur le même serveur).

➢ La valeur par défaut du serveur est **Fiable (authentification Windows)** (si vous êtes déjà connecté). Vous pouvez également sélectionner **Spécifier le nom d'utilisateur et le mot de passe (Authentification SQL)** si vous disposez d'identifiants valides qui permettent d'accéder à la base de données et si vous préférez l'authentification SQL. Si vous choisissez cette dernière, assurez-vous de TESTER la connexion à la base de données en cliquant sur **Tester la connexion**.

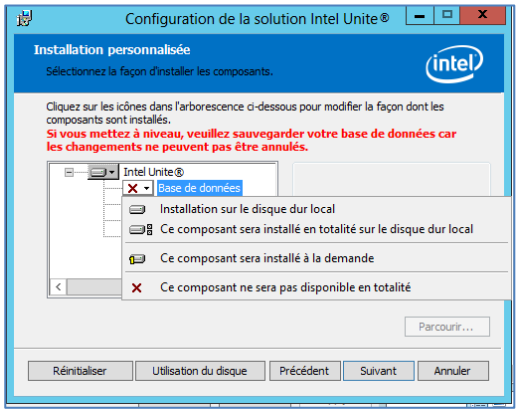
➢ Il existe un nouveau paramètre du portail Web administrateur : la valeur de l'**hôte (FQDN)** ou le nom de l'URL de redirection doit être indiqué ici. Le programme d'installation utilisera le FQDNUGS du serveur où il s'exécute.

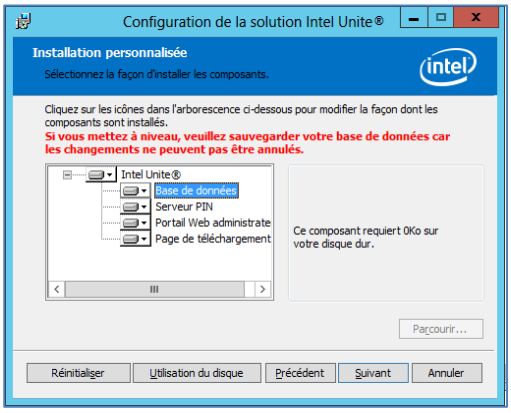
➢ Dans le champ **Informations de configuration et de connexion de la base de données**, vous devez créer un mot de passe pour **UniteServiceUser**, qui est utilisé pour accéder à la nouvelle base de données intitulée UniteServer. **Confirmez le mot de passe** dans la boîte de dialogue suivante.

➢ Le mot de passe doit comporter au moins 8 caractères, dont au moins un caractère en majuscule, un caractère en minuscule, un chiffre et un symbole.



- Cliquez sur **Suivant** pour passer à la fenêtre **Installation personnalisée** afin de sélectionner des fonctionnalités. Développez les fonctionnalités de la base de données et sélectionnez **Installation sur le disque dur local** ou **Ce composant sera installé en totalité sur le disque dur local**. Cette action crée la base de données sur le serveur SQL indiqué à l'étape précédente.

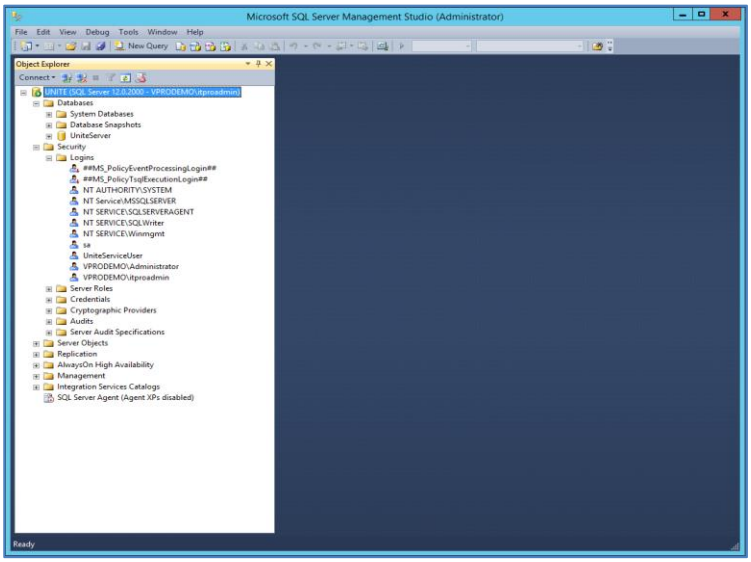




- Cliquez sur **Suivant** pour vérifier la sélection de fonctionnalités et lancez l'installation en cliquant sur **Installer**.
- Cliquez sur **Terminer** pour achever l'installation.
- Vous avez installé le serveur d'entreprise. Passez à la section suivante pour installer le concentrateur.

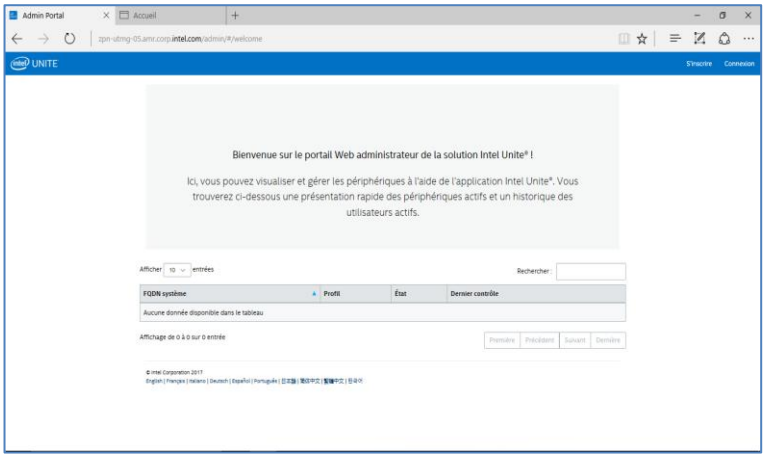
Optionnel :

- Pour vérifier que la base de données UniteServer a été créée à l'aide de SQL Management Studio, ouvrez SQL Management Studio sur votre serveur et connectez-vous au serveur SQL. Développez les bases de données dans le volet de gauche et assurez-vous que la base de données UniteServer a été créée.



- Vérifiez que l'installation a abouti en accédant au portail administrateur (s'il est installé sur le serveur avec la base de données et le serveur PIN) en suivant ce lien : https://<nomdevotreserveur>/admin

  Vous pouvez vous connecter à votre compte si vous en avez un. En cas de nouvelle installation logicielle, vous pouvez utiliser le compte administrateur par défaut. Le système vous invitera à en modifier le mot de passe avant de continuer.
  Utilisateur par défaut : admin@server.com
  Mot de passe : Admin@1

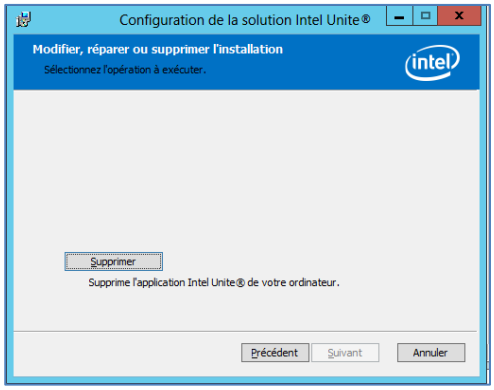


Remarque : si un message d'erreur s'affiche lorsque vous accédez au portail administrateur, consultez la section Dépannage.

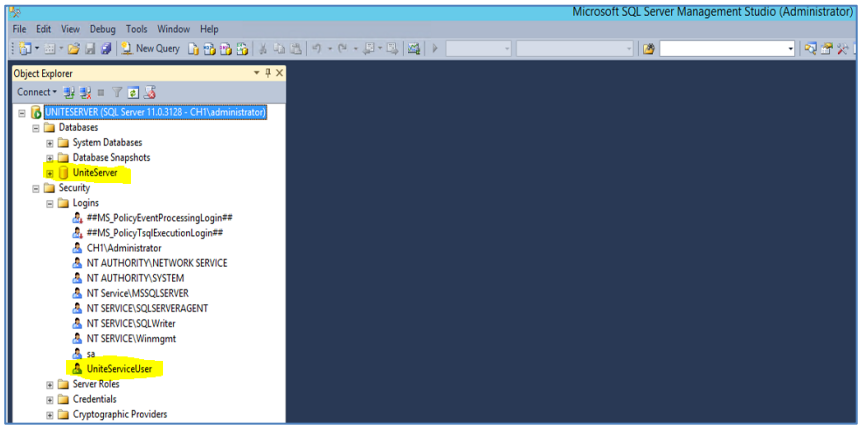
4.4 Désinstallation de l'application Intel Unite®

Si vous avez besoin de désinstaller l'application, vous devez également supprimer la base de données UniteServer et l'identifiant de connexion UniteServiceUser précédemment créés pour éviter tout conflit au sein de l'application. Avant de le faire, **assurez-vous d'avoir effectué une sauvegarde de votre base de données**.

1. Lancez le programme d'installation **Intel Unite Server.mui**.
2. Cliquez sur **Supprimer**, puis sur **Suivant** pour continuer.



3. Accédez à *Microsoft SQL Server Management Studio* et supprimez manuellement la base de données SQL **UniteServer** ainsi que le compte **UniteServiceUser**. Observez les zones en surbrillance de l'image ci-dessous.



5 Installation du concentrateur

5.1 Pré-installation du concentrateur

L'application Intel Unite® nécessite une exception dans le pare-feu du concentrateur pour se connecter et communiquer avec le serveur d'entreprise, car le concentrateur doit pouvoir localiser le serveur d'entreprise et s'y connecter.

Lorsque vous exécutez le programme d'installation du concentrateur, celui-ci vous invite à fournir vos informations de connexion au serveur et vous donne la possibilité de contourner la recherche manuelle (**Spécifier le serveur** dans le processus d'installation) afin de récupérer des informations depuis l'enregistrement de service DNS. L'exécution du programme d'installation du concentrateur a pour effet d'éditer le fichier ServerConfig.xml.

Selon la méthode choisie pour la recherche de code PIN, vous devez savoir si vous souhaitez utiliser l'option **Rechercher automatiquement le serveur** ou **Spécifier le serveur** lors de l'exécution de l'installation.

Si vous savez que l'enregistrement de service DNS existe, vous pouvez sélectionner **Rechercher automatiquement le serveur**. Si vous n'êtes pas sûr, utilisez l'option **Spécifier le serveur** (recherche manuelle) : vous devez connaître le nom d'hôte du serveur d'entreprise.

Si vous avez édité le fichier ServerConfig.xml avec la clé publique (voir la section suivante Clé publique), vous n'avez pas besoin de saisir de nouveau la clé pour l'installation du client et du concentrateur.

Remarque : si un serveur est défini dans le fichier ServerConfig.xml, il aura priorité sur l'enregistrement de service DNS.

5.1.1 Clé publique

La clé publique est facultative. Elle spécifie comment le client ou le concentrateur communique avec le serveur d'entreprise. Si elle est vierge ou non spécifiée, le concentrateur et le client valideront la racine de confiance. Si l'application n'accepte pas le certificat, elle invitera l'utilisateur à effectuer une saisie.

La clé publique devrait être utilisée lors de l'exécution de l'installation du concentrateur et du client. Vous aurez besoin de cette clé lors de l'exécution des programmes d'installation du concentrateur et du client. Pour obtenir la clé publique, rendez-vous sur la page : https://nomdevotreserveur/unite/ccservice.asmx

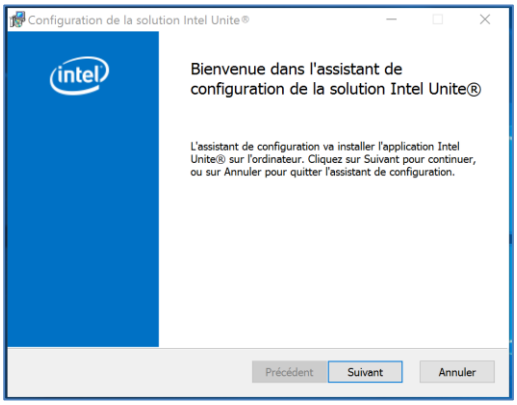
Dans la barre d'URL, cliquez sur le cadenas pour afficher les informations de certificat. Allez dans « Détails », cliquez sur « Afficher tout », faites défiler jusqu'à « Clé publique », puis cliquez sur la clé publique pour l'afficher. Vous pouvez également copier la valeur et la coller dans le fichier ServerConfig.xml.

Assurez-vous de supprimer les espaces de la chaîne après avoir collé la valeur dans le fichier ServerConfig. Si vous avez édité le fichier ServerConfig.xml avec la clé publique, vous n'avez pas besoin de saisir de nouveau la clé pour l'installation du client et du concentrateur. Consultez l'annexe B pour obtenir un exemple de fichier ServerConfig.xml.

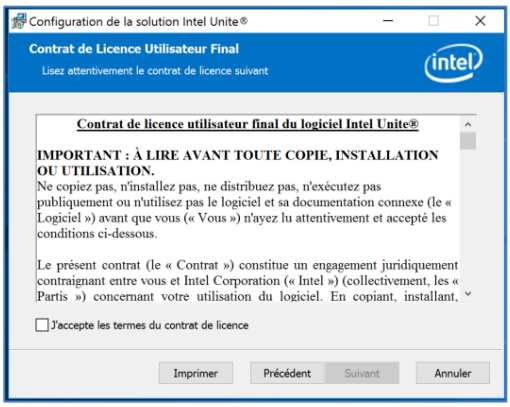
5.2 Installation du concentrateur

- Localisez le dossier du programme d'installation et exécutez le programme d'installation du concentrateur : **Intel Unite Hub.msi**.

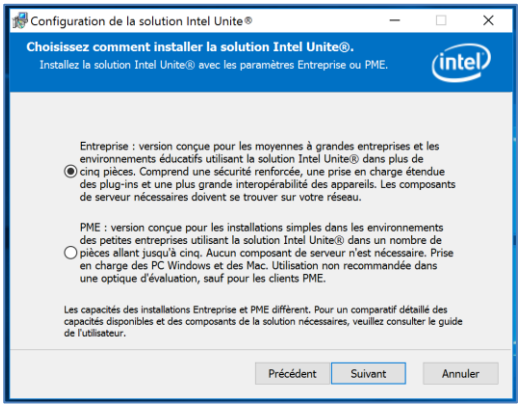
- Cliquez sur **Suivant** pour continuer.



- Cliquez sur **Suivant** après avoir sélectionné la case **J'accepte les termes du contrat de licence**.

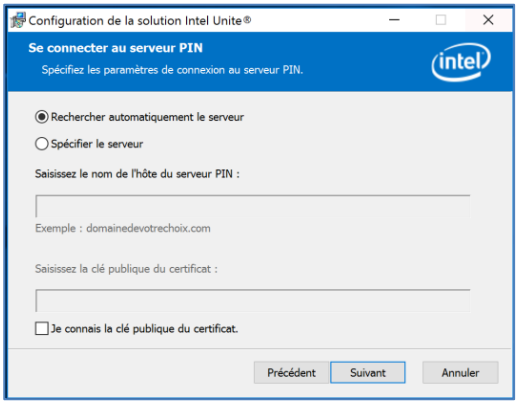


- Sélectionnez **Entreprise** et cliquez sur **Suivant**.

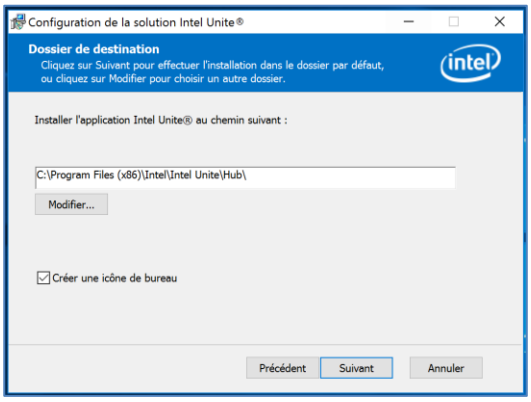


- Dans cette fenêtre, vous devez spécifier les paramètres de connexion au serveur PIN. Les options disponibles sont les suivantes :
  - **Rechercher automatiquement le serveur** : il s'agit de l'option recommandée (par défaut).
  - **Spécifier le serveur** : à cette étape, vous devez connaître le nom de l'hôte du le serveur d'entreprise.
    - **Saisissez le nom de l'hôte du serveur PIN.**
    - Saisissez la **clé publique de certificat** si vous avez coché la case **Je connais la clé publique du certificat**.

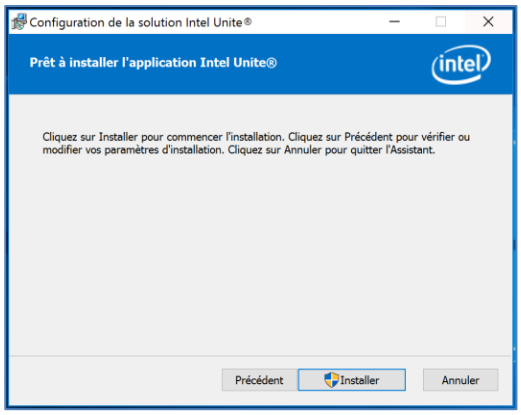
  Faites votre choix et cliquez sur **Suivant**.



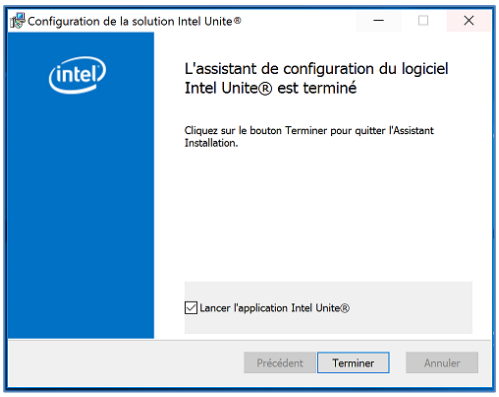
- La fenêtre **Dossier de destination** s'ouvre et affiche le dossier par défaut où sera installé le concentrateur. Vous pouvez modifier le dossier de destination si vous le souhaitez ou conserver l'emplacement par défaut. À cette étape, vous pouvez également créer une icône de bureau. Cliquez sur **Suivant** pour continuer.



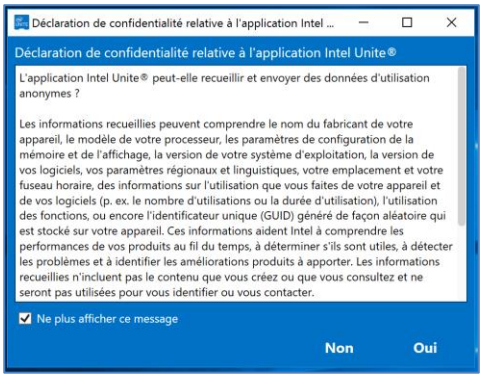
- À ce stade, vous pouvez revenir en arrière pour vérifier vos paramètres ou cliquer sur **Installer** pour continuer.



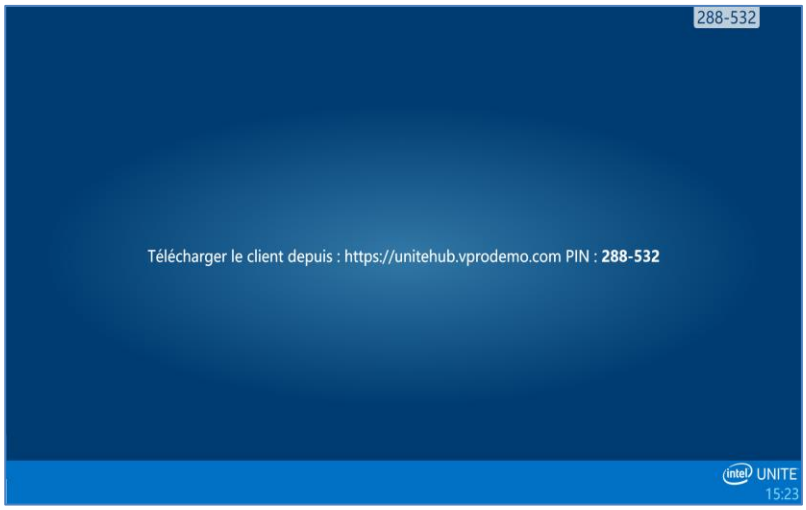
- Une fois l'installation terminée, la fenêtre **L'assistant de configuration du logiciel Intel Unite® est terminé** s'ouvre. Cliquez sur **Terminer** pour mettre fin au processus d'installation.



  - Lorsque vous ouvrez l'application pour la première fois, la **déclaration de confidentialité relative à l'application Intel Unite®** s'affiche.



  - La déclaration de confidentialité relative à l'application Intel Unite® est utilisée pour recueillir des données d'utilisation anonymes. Intel cherche en permanence à améliorer ses produits et souhaiterait recueillir des données à cette fin. Veuillez sélectionner **OUI** ou **NON**, et cochez la case si vous ne souhaitez pas que cette boîte de dialogue s'affiche de nouveau.
  - Vous verrez à présent s'afficher un code PIN sur votre affichage ou moniteur. Il s'agit du code PIN dont vous aurez besoin pour connecter les clients au concentrateur. (Consultez la rubrique Dépannage si le code PIN n'apparaît pas.)



5.3 Configuration du concentrateur

Les options de configuration des concentrateurs qui exécutent le logiciel Intel Unite® peuvent être modifiées depuis le portail administrateur. Le portail administrateur contient un profil par défaut où apparaissent les paramètres de configuration par défaut s'appliquant à tous les concentrateurs qui se connectent au serveur d'entreprise. Les options de configuration sont appliquées aux concentrateurs après l'établissement de la connexion entre le concentrateur et le serveur d'entreprise. Les paramètres sont mis à jour à chaque connexion du concentrateur. De plus, la plupart des paramètres du concentrateur peuvent être personnalisés en fonction des besoins de votre entreprise : par exemple, chaque concentrateur peut afficher une image, une couleur ou une taille de code PIN différente, ou contenir des plug-ins différents. Consultez la section Guide du portail administrateur pour en savoir plus sur la configuration du concentrateur.

5.4 Pratiques recommandées relatives au concentrateur

Afin d'assurer la meilleure expérience possible à l'utilisateur final, le concentrateur doit être configuré de sorte à pouvoir toujours être utilisé. Les alertes système ou fenêtres pop-up qui s'affichent à l'écran doivent être supprimées. Les pratiques recommandées sont, entre autres, les suivantes :

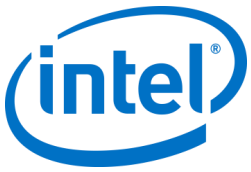
- Windows doit automatiquement se connecter au domaine ou à l'utilisateur que l'application Intel Unite® exécutera.
- Les économiseurs d'écran doivent être désactivés.
- Le système doit être configuré de sorte à ne jamais se mettre en veille.
- Le système doit être configuré de sorte à ne jamais se déconnecter.
- L'affichage ne doit jamais se désactiver.
- Les alertes système doivent être supprimées.

5.5 Sécurité des concentrateurs

L'administrateur des concentrateurs doit s'assurer que les pratiques de sécurité recommandées sont suivies sur chaque concentrateur. Si l'utilisateur local se connecte automatiquement, il convient de s'assurer qu'il n'exécute pas le programme avec des droits d'administrateur.

5.6 Plug-ins

L'application Intel Unite® prend en charge l'utilisation de plug-ins. Les plug-ins sont des éléments logiciels qui élargissent les fonctionnalités de l'application, améliorant ainsi l'expérience des utilisateurs. Les plug-ins peuvent être propres à chaque concentrateur. Veuillez consulter le guide spécifique au plug-in que vous



souhaitez installer pour obtenir plus d'informations. Les plug-ins suivants sont actuellement disponibles pour l'application Intel Unite® :

Plug-in d'accès invité en mode protégé : ce plug-in permet à un ordinateur de se connecter à un concentrateur sans avoir à être sur le même réseau d'entreprise et sans validation du code PIN du serveur d'entreprise. Le concentrateur crée un réseau ad hoc/hébergé (point d'accès) grâce auquel un client Intel Unite® peut se connecter.

Plug-in pour Skype Entreprise : ce plug-in permet d'ajouter les participants d'une réunion en ligne sur Skype à une session avec l'application Intel Unite®. Le plug-in s'exécute sur le concentrateur du logiciel Intel Unite® et gère un compte de messagerie propre à chaque instance.

Plug-in de télémétrie (version logicielle 3.x) : ce plug-in permet au serveur d'entreprise d'accepter et d'afficher les données du concentrateur. Enterprise Server v3.0 au minimum est requis (Build 3.0.38.44). Il convient de noter que sur la version logicielle 4.0, cette fonctionnalité a été ajoutée à la solution : il n'est donc pas nécessaire d'ajouter le plug-in.

Plug-in pour Whiteboard : lors de l'utilisation d'un écran tactile, ce plug-in permet à l'écran sur lequel s'exécute l'application Intel Unite® de se convertir en tableau blanc pour une utilisation par les participants présents dans la salle : ceux-ci peuvent faire des annotations sur l'écran et envoyer le contenu final aux autres participants à la séance.

De plus, il existe un kit de développement logiciel permettant d'écrire des plug-ins :
Kit de développement logiciel (SDK) : guide de l'interface de l'application permettant d'aider les développeurs ou les personnes souhaitant ajouter de nouvelles fonctionnalités à l'application Intel Unite®.

5.6.1 Remarques relatives à l'installation du plug-in

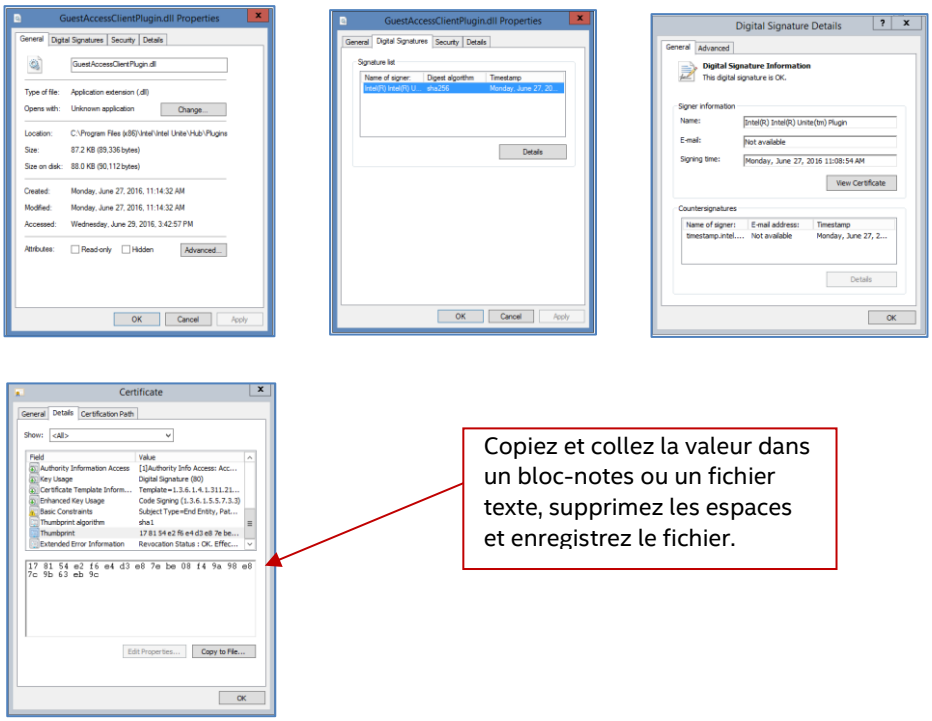
Chaque plug-in est installé par défaut dans le sous-répertoire des plug-ins du répertoire d'installation [Program Files(x86) \Intel\Intel Unite\Hub\Plugins\PluginName (Plugin.dll)]. Les plug-ins sont énumérés au démarrage de l'application. En cas d'ajout d'un plug-in, l'application doit être redémarrée.
Avant d'installer le plug-in, vérifiez qu'il est compatible avec la version cible de votre solution Intel Unite® (veuillez consulter le guide du plug-in, car les exigences minimales varient).
Vous devez également veiller à obtenir et ajouter la valeur de hachage du certificat pour chaque plug-in utilisé sur le portail Web administrateur.
REMARQUE : vous pouvez utiliser la valeur par défaut de la clé pour configurer un environnement de test, mais l'utilisation de cette valeur n'est pas recommandée dans un environnement de production.

5.6.2 Valeur de hachage du certificat du plug-in

Suivez ces étapes pour trouver la valeur de la clé de hachage du certificat de votre plug-in :

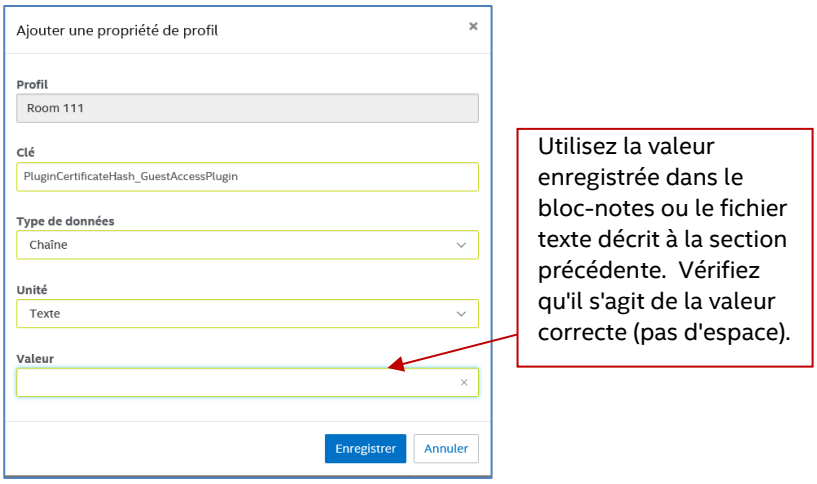
- Repérez le plug-in dans le dossier des plug-ins, cliquez avec le bouton droit de la souris sur ***Plugin.dll** et sélectionnez **Propriétés** (p. ex. GuestAccessClientPlugin.dll).
- Lorsque la fenêtre **Propriétés** du plug-in s'ouvre, accédez à l'onglet **Signatures numériques**, puis cliquez sur Ouvrir.
- Sélectionnez **Intel Unite Plugin** et cliquez sur **Détails**.
- Dans la fenêtre **Détails de la signature numérique**, cliquez sur **Afficher le certificat.**
- Dans la fenêtre **Certificat**, sélectionnez l'onglet **Détails** et faites défiler la page vers le bas jusqu'à **Empreinte numérique**.

- Sélectionnez **Empreinte numérique**. Une fois que la valeur s'affiche, copiez et collez-la dans un bloc-notes ou un fichier texte, supprimez les espaces et enregistrez le fichier.
- Cette valeur de clé vous servira au moment de créer le profil de votre plug-in. Il est possible de créer et saisir la valeur de la clé après la création du profil. Consultez la section suivante pour en savoir plus.



5.6.3 Ajout du hachage du certificat à un plug-in sur le portail Web d'administration

Accédez au portail Web d'administration, puis sous **Groupes,** sélectionnez le profil sur lequel vous souhaitez activer le plug-in.
Dans la fenêtre Profil, cliquez sur **Ajouter une propriété de profil** et saisissez ce qui suit :

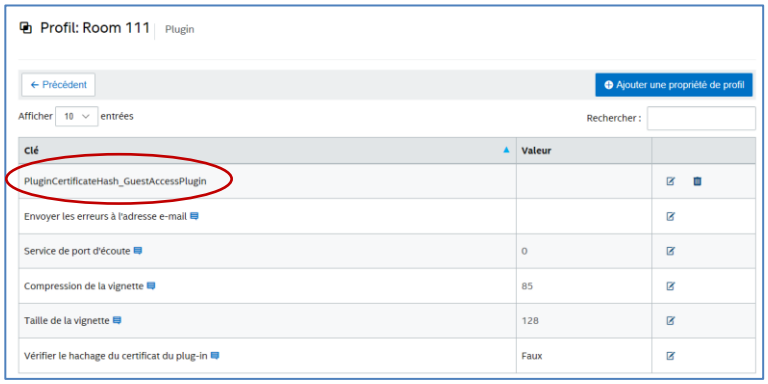


- **Clé** : PluginCertificateHash_XXX

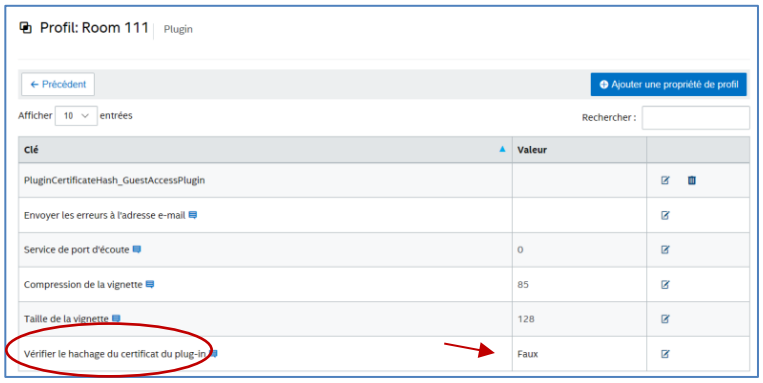
- XXX est le nom du plug-in pour lequel le hachage est ajouté, par exemple GuestAccessPlugin. À des fins d'identification, il est conseillé d'utiliser le nom du plug-in qui correspond au hachage.

- **Type de données :** chaîne
- **Unité :** texte
- **Valeur :** utilisez la valeur de l'empreinte enregistrée dans le bloc-notes ou le fichier texte mentionné dans la section *Valeur de hachage du certificat du plug-in.* La valeur de la clé peut également être saisie après la création de la clé.

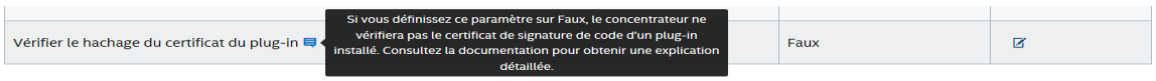
Cliquez sur **Enregistrer**. Vous pouvez mettre à jour les valeurs ultérieurement en sélectionnant le lien **Modifier**.
La nouvelle clé s'affichera dans la fenêtre Profil.



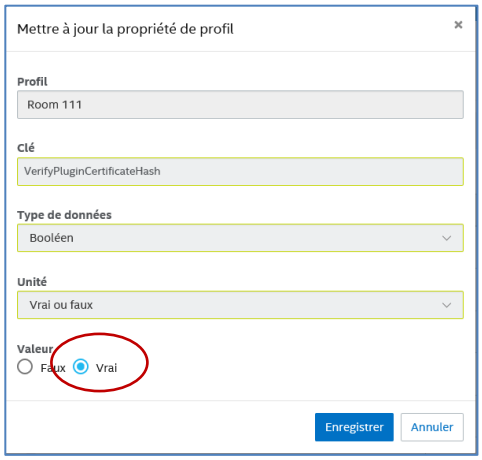
Il vous faut également activer la clé **Vérifier le hachage du certificat du plug-in** en la positionnant sur Vrai (la valeur par défaut est Faux).



Vous pouvez choisir d'activer ou de désactiver le plug-in en sélectionnant Vrai ou Faux. Veuillez noter que les valeurs de clé assurent la validité du plug-in.



Cliquez sur le lien Modifier pour positionner la valeur sur **Vrai**, puis **Enregistrer**.



Les paramètres du plug-in sont désormais activés.

6 Installation du client

6.1 Pré-installation du client

Le client doit pouvoir localiser le serveur d'entreprise et s'y connecter. L'application Intel Unite® nécessite une exception dans le pare-feu client pour se connecter et communiquer avec le serveur d'entreprise. Lorsque vous exécutez le programme d'installation du client, celui-ci vous invite à fournir vos informations de connexion au serveur et vous donne la possibilité de contourner la recherche manuelle (**Spécifier le serveur** dans le processus d'installation) afin de récupérer des informations depuis l'enregistrement de service DNS. Lors de l'exécution du programme d'installation, il édite le fichier ServerConfig.xml.

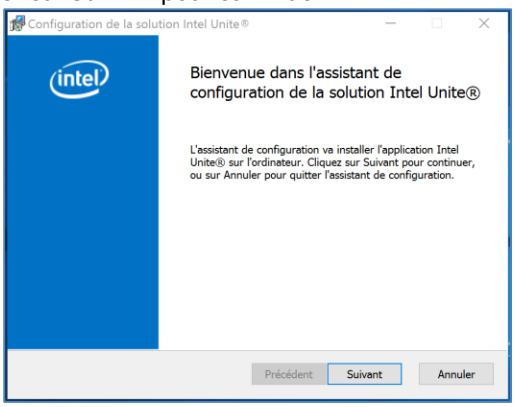
Selon la méthode choisie pour la recherche de code PIN, vous devez savoir si vous souhaitez utiliser l'option **Rechercher automatiquement le serveur** ou **Spécifier le serveur** lors de l'exécution de l'installation.
Si vous savez que l'enregistrement de service DNS existe, vous pouvez sélectionner **Rechercher automatiquement le serveur**. Il est préférable d'utiliser la recherche automatique afin d'éviter des erreurs de saisie. Si vous n'êtes pas sûr, utilisez l'option **Spécifier le serveur** (recherche manuelle), pour laquelle vous devez connaître le nom d'hôte du serveur d'entreprise.

Remarque : si un serveur est défini dans le fichier ServerConfig.xml, il aura priorité sur l'enregistrement de service DNS.

Appareils clients mobiles : tous les appareils clients (y compris les appareils iOS et Android) doivent être connectés au réseau d'entreprise ou utiliser un VPN configuré de manière adéquate. Il se peut que les tablettes et les téléphones normalement utilisés à des fins personnelles et qui ne sont pas connectés au réseau d'entreprise, mais au réseau de leur propre opérateur, ne puissent pas rejoindre une session de l'application Intel Unite® : il est possible en effet que vous disposiez d'un pare-feu d'entreprise qui empêche une telle connexion. Consultez la section Appareils clients mobiles pour obtenir plus d'informations.

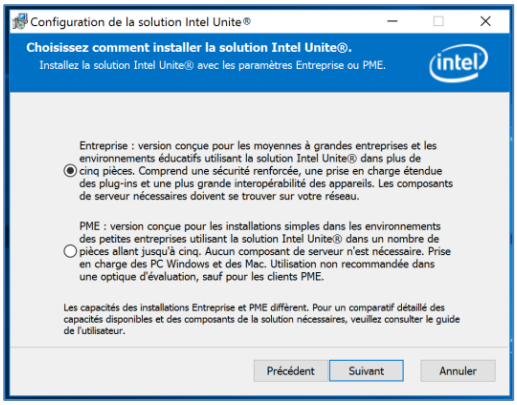
6.2 Installation du client Windows

- Localisez le dossier d'installation et exécutez l'assistant d'installation du client : **Intel Unite Client.mui.msi.** Cliquez sur **Suivant** pour continuer.

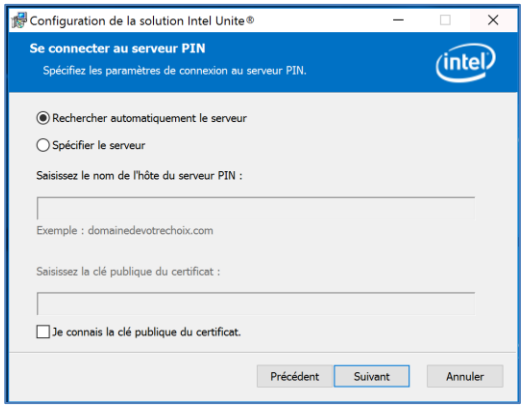


- Cochez la case **J'accepte les termes du contrat de licence** et cliquez sur **Suivant**.

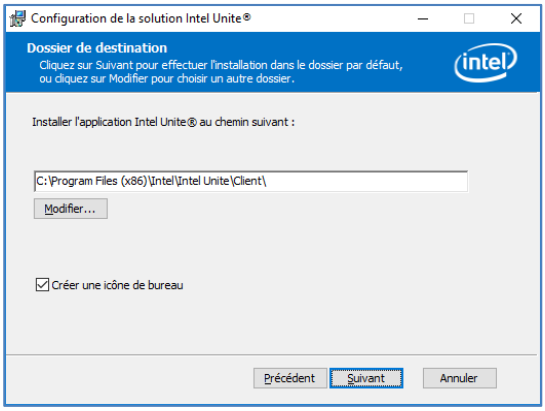
- Sélectionnez **Entreprise** et cliquez sur **Suivant**.



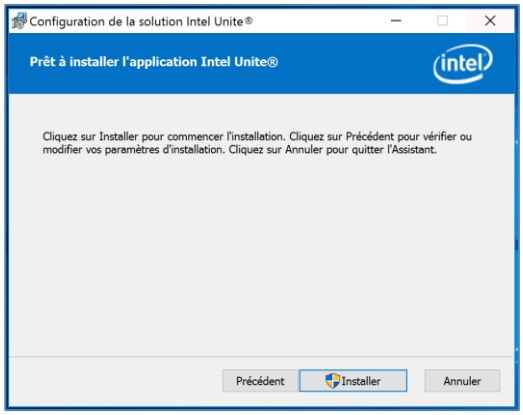
- Dans cette fenêtre, vous devez spécifier les paramètres de connexion au serveur PIN. Les options sont les suivantes :
  - **Rechercher automatiquement le serveur** : il s'agit de l'option la plus pratique (par défaut).
  - **Spécifier le serveur** : à cette étape, vous devez connaître le nom de l'hôte du serveur d'entreprise.
    - **Saisissez la clé publique du certificat** : cette option s'active lorsque vous sélectionnez **Spécifier le serveur.**
    - Saisissez la **clé publique de certificat** si vous l'avez et si vous avez sélectionné cette méthode.
- Faites votre choix et cliquez sur **Suivant** pour continuer.



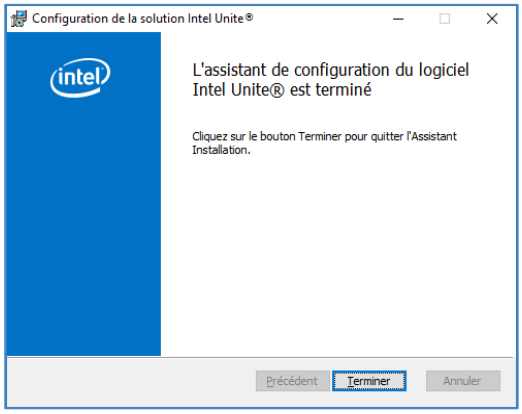
- La fenêtre **Dossier de destination** s'ouvre avec le dossier par défaut dans lequel l'application Intel Unite® est installée sur le client. Vous pouvez modifier le dossier de destination si vous le souhaitez ; sinon, conservez l'emplacement par défaut.



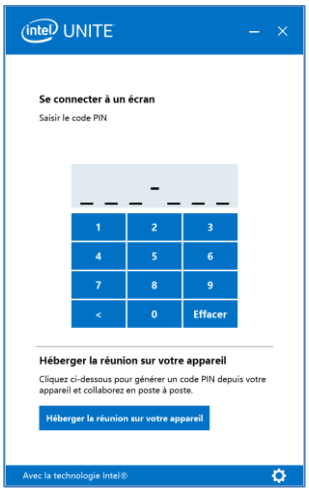
  - Vous pouvez revenir en arrière pour vérifier vos paramètres ou cliquer sur **Installer** pour continuer.



  - Une fois l'installation terminée, la fenêtre **L'assistant de configuration du logiciel Intel Unite® est terminé** s'ouvre. Cliquez sur **Terminer**.



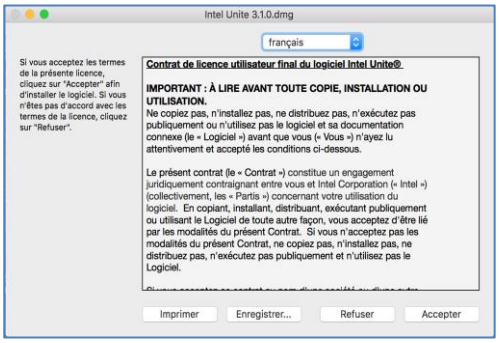
- La fenêtre **Se connecter à un écran** suivante s'affiche :



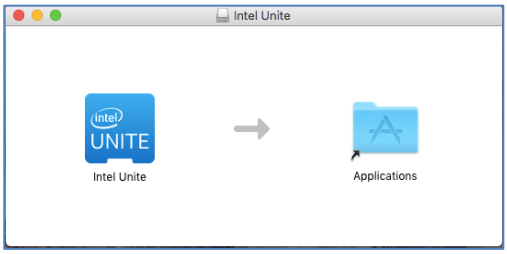
- Pour vous connecter au concentrateur, saisissez le code PIN qui s'affiche sur le moniteur ou l'écran. Par défaut, le code PIN change toutes les cinq minutes.
- Veuillez consulter le **Guide d'utilisation de la solution Intel Unite®** pour en savoir plus sur les fonctionnalités et l'utilisation de la solution.

6.3 Installation du client macOS

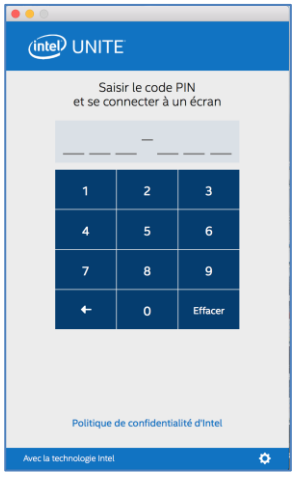
- Repérez le fichier **Intel Unite macOS X,X.dmg** et téléchargez le logiciel sur votre client Mac. Double-cliquez sur le fichier pour extraire l'application.
- Vous serez invité à accepter les conditions du **Contrat de licence utilisateur final**. Cliquez sur **Accepter** pour continuer.



- Une fois l'application extraite, faites-la glisser dans le dossier Applications.



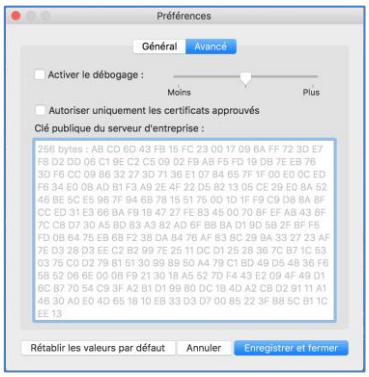
- Accédez au dossier Applications et repérez l'application. Cliquez dessus pour la lancer.
- L'écran **Saisir le code PIN et se connecter à un écran** s'ouvre. Vous pouvez vous connecter au concentrateur en saisissant le code PIN qui s'affiche sur le moniteur ou l'écran pour démarrer le partage.



- Veuillez consulter le **Guide d'utilisation de la solution Intel Unite®** pour en savoir plus sur les fonctionnalités et l'utilisation de la solution.

Remarque : l'application utilise la découverte automatique DNS (enregistrement de service DNS) pour localiser le serveur d'entreprise. Un serveur d'entreprise par défaut peut également être spécifié en

modifiant les paramètres com.intel.Intel-Unite.plist du dossier de l'utilisateur ~/Bibliothèque/Préférences :
par défaut, il s'agit de com.intel.Intel-Unite EnterpriseServer myServer.mydomain.myTLD. Pour plus d'informations, consultez la section *Solution Intel Unite® pour macOS* de ce guide.
Vous pouvez également modifier le serveur d'entreprise auquel l'application doit se connecter. Cliquez sur l'icône en forme d'engrenage dans le coin inférieur droit de l'**écran de connexion** pour accéder aux **paramètres**.
Deux onglets sont disponibles :

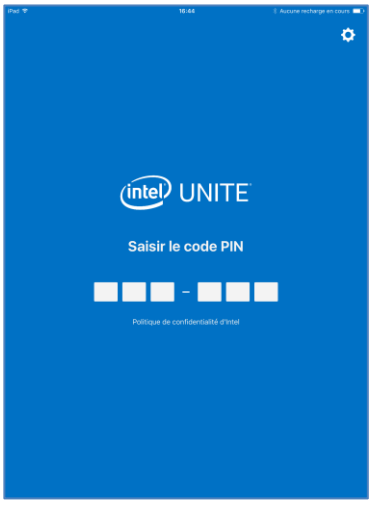


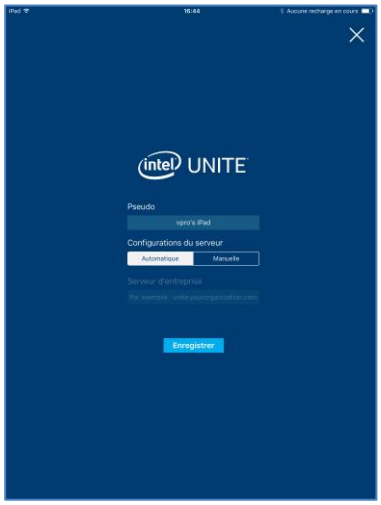
Général : vous pouvez saisir le nom, l'adresse e-mail et l'avatar de l'utilisateur. Vous pouvez également indiquer si la machine client doit se connecter automatiquement au serveur d'entreprise (par défaut) ou après saisie d'un chemin d'accès défini au serveur.
Avancé : cet onglet vous permet d'**activer le débogage** ou d'indiquer si vous autorisez uniquement les **certificats approuvés**.

6.4 Installation du client iOS

L'application est compatible avec tous les iPads sauf l'iPad original de 2010.

- Sur votre client iOS (p. ex. sur votre iPad), accédez à l'Apple App Store et téléchargez le logiciel Intel Unite® propre à votre client.
- Une fois l'application téléchargée, ouvrez-la.
- Cliquez sur l'icône en forme d'engrenage dans le coin supérieur droit pour accéder aux **Paramètres** et saisissez les informations demandées.





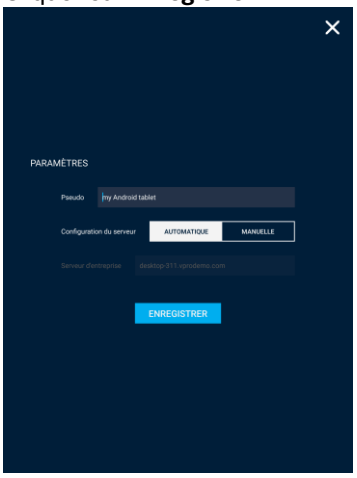
- Sous **Paramètres**, saisissez le pseudo et les informations du serveur.

- Vous pouvez sélectionner **Automatique** pour détecter le serveur. Si vous souhaitez vous connecter à un serveur spécifique, cliquez sur **Manuelle** et indiquez le serveur auquel vous souhaitez vous connecter.
- Cliquez sur **Enregistrer**.
- Vous pouvez vous connecter au concentrateur en saisissant le code PIN qui s'affiche sur le moniteur ou l'écran, et démarrer le partage.
- Veuillez consulter le **Guide d'utilisation de la solution Intel Unite®** pour en savoir plus sur les fonctionnalités et l'utilisation de la solution.

6.5 Installation du client Android

- Sur votre appareil Android, accédez à la boutique d'applications Google et téléchargez le logiciel Intel Unite® propre à votre client.
- Une fois l'application téléchargée, ouvrez-la.
- Cliquez sur l'icône en forme d'engrenage dans le coin supérieur droit pour accéder aux **Paramètres** et saisissez les informations demandées.

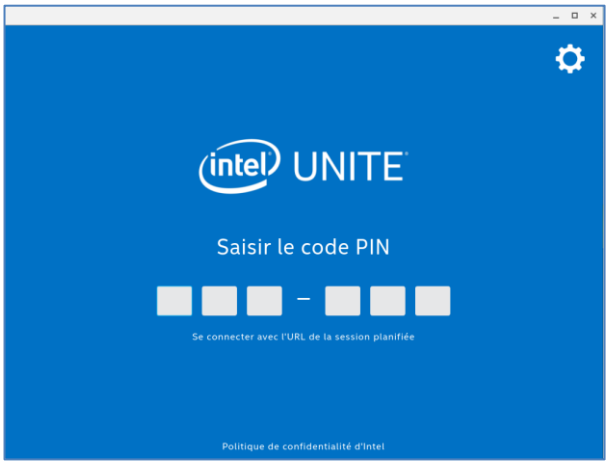
- Sous **Paramètres**, saisissez votre pseudo et les informations du serveur.
- Vous pouvez sélectionner **Automatique** pour détecter le serveur. Si vous souhaitez vous connecter à un serveur spécifique, cliquez sur **Manuelle** et indiquez le serveur auquel vous souhaitez vous connecter.
- Cliquez sur **Enregistrer**.



- Vous pouvez vous connecter au concentrateur en saisissant le code PIN qui s'affiche sur le moniteur ou l'écran, et démarrer le partage.
- Veuillez consulter le **Guide d'utilisation de la solution Intel Unite®** pour en savoir plus sur les fonctionnalités et l'utilisation de la solution.

6.6 Installation du client Chrome

- Sur votre appareil Chrome, accédez à la boutique d'applications Google et téléchargez le logiciel Intel Unite® propre à votre client.
- Une fois l'application téléchargée, ouvrez-la.
- Cliquez sur l'icône en forme d'engrenage dans le coin supérieur droit pour accéder aux **Paramètres** et saisissez les informations demandées.



- Sous Paramètres, saisissez le nom de l'écran, l'e-mail et les informations du serveur. Vous pouvez sélectionner **Automatique** pour détecter le serveur. Si vous souhaitez vous connecter à un serveur spécifique, cliquez sur **Manuelle** et indiquez le serveur auquel vous souhaitez vous connecter.
- Cliquez sur **Enregistrer les paramètres**.

Vous pouvez vous connecter au concentrateur en saisissant le code PIN qui s'affiche sur le moniteur ou l'écran, et démarrer le partage.
Veuillez consulter le **Guide d'utilisation de la solution Intel Unite®** pour en savoir plus sur les fonctionnalités et l'utilisation de la solution.

6.7 Configuration du client

Les paramètres de configuration du client peuvent être modifiés à partir du portail administrateur. Le portail administrateur contient un profil par défaut qui contient les paramètres de configuration par défaut s'appliquant à tous les clients qui se connectent au serveur. Les options de configuration sont propagées au client après l'établissement de la connexion entre le client et le serveur d'entreprise. Les paramètres sont mis à jour à chaque connexion d'un client.
Veuillez consulter la rubrique Configuration de profil pour comprendre les options de configuration.

7 Installation avancée

7.1 Installateurs scriptés

Cette rubrique fournit des informations sur l'exécution silencieuse des programmes d'installation, sans que des menus ou des fenêtres n'apparaissent. Ainsi, les paramètres de propriété seront transférés au programme d'installation via la ligne de commande.
Pour exécuter les programmes d'installation en mode silencieux, ouvrez l'invite de commande et utilisez la ligne de commande suivante :
msiexec /i "CHEMIN_VERS_CLIENT_MSI" PARAMETER=VALUE PARAMETER=VALUE ... /qn /l* “CHEMIN_VERS_LOG”

- L'indicateur /i se réfère au MSI spécifié pour l'installation. « CHEMIN_VERS_CLIENT_MSI » est le nom de fichier du programme d'installation que vous appelez.
- « PARAMETER=VALUE PARAMETER=VALUE ... » est une liste des paramètres indiqués dans le tableau ci-dessous.
- L'indicateur /qn exécutera le programme d'installation en mode silencieux.
- L'indicateur /l* transmet le journal de sortie au fichier de journal que vous avez indiqué.

REMARQUE : vous pouvez voir toutes les options du fichier **msiexec** en exécutant la commande suivante : msiexec /?
Vous trouverez ci-dessous une liste complète des paramètres de propriété qui peuvent être transmis dans chaque programme d'installation :

Paramètres d'installation du serveur	Description
DBHOSTNAME = "local" ou "{IP}" ou "{serveur},{port}" (par défaut, local)	Nom de l'hôte du serveur Microsoft SQL. Il s'agit de l'emplacement où le programme d'installation crée la base de données UniteServer et ajoute le compte de service de la base de données. Si vous installez la base de données sur la machine actuelle, il n'est pas nécessaire d'inclure ce paramètre, car sa valeur par défaut est « local ».
DBLOGONTYPE = "WinAccount" ou "SqlAccount" → par défaut sur WinAccount	Indique le type d'ouverture de session pour l'accès au serveur Microsoft SQL. Les options sont l'authentification Windows ou l'authentification SQL.
DBUSER = "{nom d'utilisateur SQL}" DBPASSWORD = "{mot de passe SQL}"	Si le type d'ouverture de session est SqlAccount, fournissez le nom d'utilisateur et le mot de passe. REMARQUE : ce compte doit avoir la permission d'ajouter la base de données et de créer le compte de service de la base de données.
DBLOGONPASSWORD = "{mot de passe du compte de service}"	Mot de passe qui sera utilisé par le compte de service pour se connecter à la base de données UniteServer.
DBLOGONPASSWORDCONF = "{mot de passe du compte de service}"	Cette variable doit avoir la même valeur que celle indiquée dans DBLOGONPASSWORD.
Paramètres de sélection des fonctionnalités du serveur	**Description**

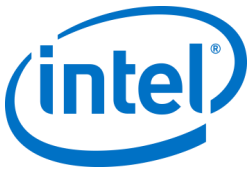
ADDLOCAL = "ALL"	Il n'existe que deux options : ALL = installe la base de données et le serveur PIN, le portail administrateur et la page de téléchargement. (Ne pas indiquer cette variable) = installe le serveur PIN, le portail administrateur et la page de téléchargement.
Paramètres d'installation du client et du concentrateur	**Description**
PINSERVERLOOKUPTYPE = "Lookup" ou "Manual" Par défaut, Lookup	Spécifie la manière dont l'application trouvera le serveur PIN. L'option Lookup utilisera l'enregistrement de service DNS, tandis que l'option Manual requiert la saisie des paramètres PINSERVER.
PINSERVER = "{nom de l'hôte}"	Nom d'hôte du serveur auquel se connecter.
CERTKEYCHECKED = "1" ou "0" Par défaut : 0	Ce paramètre est facultatif. 0 = Ne pas vérifier le hachage de la clé de certificat 1 = Vérifier le hachage de la clé de certificat, la CERTKEY doit également être indiquée.
CERTKEY = "{clé de certificat}"	Ce paramètre est facultatif. Saisissez la clé publique de certificat du serveur PIN.
SHORTCUTS	Facultatif. Utilisez « 1 » pour placer les icônes de raccourci sur le Bureau.
INSTALLTYPE = deux valeurs possibles, « Enterprise » et « StandAlone ».	Si INSTALLTYPE est défini sur « Enterprise », le client ou le concentrateur s'installera en mode entreprise. Si INSTALLTYPE est défini sur « StandAlone », le client ou le concentrateur s'installera en mode autonome.
SKIP_EXTENDED_DISPLAY= 1 ou 0 Par défaut : 0	0 = Faux 1 = Vrai

7.2 Clés de registre

Les clés de registre sont générées dans le registre lors de l'exécution des programmes d'installation et de l'application. Les valeurs de certaines de ces clés peuvent être modifiées en fonction du résultat désiré. Consultez la liste ci-dessous pour comprendre les clés générées par l'application Intel Unite®.

Clés de registre : (current user)	Valeur	Périphérique
HKEY_CURRENT_USER\software\Intel\Unite\ ActiveConnection (DWORD)	[0 = aucun utilisateur connecté, 1 = utilisateurs connectés.]	Concentrateur

HKEY_CURRENT_USER\software\Intel\Unite\ PublicKey (Chaîne)	[clé publique de certificat de connexion]	Les deux
HKEY_CURRENT_USER\software\Intel\Unite\ CurrentPin (Chaîne)	[code PIN actuel de ce système]	Concentrateur
HKEY_CURRENT_USER\software\Intel\Unite\ DoNotShowPrivacyStatement (DWORD)	[0 = déclaration de confidentialité au démarrage, 1 = ne pas afficher la déclaration de confidentialité .]	Les deux
HKEY_CURRENT_USER\software\Intel\Unite\ HWThumbprint (Chaîne)	[hachage de HW]	Les deux
HKEY_CURRENT_USER\software\Intel\Unite\ ServicePort (DWORD)	[port d'écoute du service]	Concentrateur
HKEY_CURRENT_USER\software\Intel\Unite\ ActivePresenter	[1 = le client présente, 0 = le client ne présente pas.]	Concentrateur
HKEY_CURRENT_USER\software\Intel\Unite\PinPadWindows (DWORD)	[1 = l'application est prête pour la saisie du code PIN, 0 = cas contraire.]	Client
HKEY_CURRENT_USER\software\Intel\Unite\GuestAccess\SSID Référence : guide relatif au plug-in D'ACCÈS INVITÉ	L'utilisation d'une valeur par défaut diminuera la sécurité de l'accès invité.	Concentrateur
HKEY_CURRENT_USER\software\Intel\Unite\GuestAccess\PSK Référence : guide relatif au plug-in D'ACCÈS INVITÉ	L'utilisation d'une valeur par défaut diminuera la sécurité de l'accès invité.	Concentrateur
HKEY_CURRENT_USER\software\Intel\Unite\GuestAccess\Download Référence : guide relatif au plug-in D'ACCÈS INVITÉ	Le lien de téléchargement par défaut est http://192.168.173.1/download	Concentrateur



HKEY_CURRENT_USER\software\Intel\Unite\ShowAvToggle (DWORD) = 1 (Bouton d'activation/désactivation du mode A/V)	Mode aéro de Windows 7. Permet à l'utilisateur de passer du mode RTF à WebRTC et vice-versa.	Client
Clés de registre : (machine)	**Valeur**	**Périphérique**
HKEY_LOCAL_MACHINE\software\Intel\Unite\ HubUnlockPassword (Chaîne)	[mot de passe pour quitter l'application du concentrateur]	Concentrateur
HKEY_LOCAL_MACHINE\software\Intel\Unite\ DisableCheckCertificateChain (DWORD)	[Établi pour les certificats auto-signés. 1 = ne pas vérifier la chaîne de certificats du certificat du serveur d'entreprise.]	Les deux
HKEY_LOCAL_MACHINE\software\Intel\Unite\ DisableUsageCollection (DWORD)	[1 = bloquer la collecte des données de télémétrie]	Les deux
HKEY_LOCAL_MACHINE\software\Intel\Unite\WindowedMode (DWORD) (fonctionne uniquement en mode PME, pas en mode Entreprise.)	[1 = l'utilisateur souhaite que le concentrateur se lance en mode fenêtré (avec les boutons réduire, agrandir et fermer), 0 = cas contraire.]	Concentrateur
HKEY_LOCAL_MACHINE\software\Intel\Unite\AllowInsecureCertificates (DWORD)	[1 = la vérification de l'algorithme du certificat doit être ignorée, 0 = le certificat d'entreprise est obligé d'utiliser un certificat SHA2.]	Les deux

HKEY_LOCAL_MACHINE\software\Intel\Unite\ShowOnlyInOneMonitor (DWORD)	[Cette clé fonctionne uniquement si le mode fenêtré est défini sur 1. 1 = une seule fenêtre de code PIN s'affichera même si plusieurs écrans sont connectés.]	Concentrateur
HKEY_LOCAL_MACHINE\SOFTWARE\Intel\Unite\S4BPlugin Keywords (chaîne) = liste,de,mots-clés,séparée,par,des,virgules	Clé utilisée pour le plug-in Skype Entreprise	Concentrateur
HKEY_LOCAL_MACHINE\software\Intel\Unite\ LogFile (Chaîne)	[chemin vers le nom de fichier avec accès en écriture vers le journal de messages de débogage de runtime]	Les deux

8 Guide du portail administrateur

Le portail administrateur est le portail d'administration Web de l'application Intel Unite®. Il permet d'afficher et de gérer les appareils sur lesquels l'application Intel Unite® est installée. Il s'agit de l'un des composants installés sur le serveur d'entreprise avec le service PIN et le serveur Web pendant l'installation. (Voir la rubrique Installation du serveur d'entreprise). Le portail administrateur n'a pas besoin de se trouver sur le même serveur que la base de données, tant qu'il a accès à la base de données.

Outre les fonctionnalités supplémentaires ajoutées, l'interface du portail administrateur a été modifiée : des menus d'aide et des informations sur les fonctionnalités ont été intégrés afin de simplifier la configuration de vos concentrateurs et de vos appareils clients.

- Pour accéder au portail administrateur, ouvrez votre navigateur et suivez le lien dirigeant vers le portail, à savoir https://<nomdevotreserveur>/admin, où <nomdevotreserveur> est le nom attribué à votre serveur Intel Unite®(nom par défaut = UniteServer, soit https://uniteserver/admin).

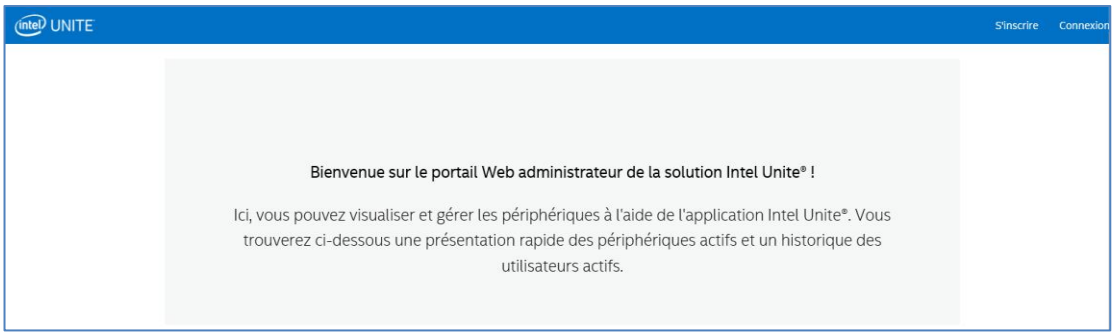
Lorsque l'administrateur informatique a exécuté les programmes d'installation des logiciels, un compte administrateur par défaut a été créé. Le nom d'utilisateur et le mot de passe correspondants sont les suivants :

- Utilisateur : admin@server.com
- Mot de passe : Admin@1

Ce compte permet un accès complet au portail administrateur et vous permet de vous connecter. Cependant, le système vous invitera à le modifier. Si vous disposez déjà d'un compte enregistré, saisissez vos informations de connexion pour accéder au portail administrateur.

8.1 Page de bienvenue du portail Web d'administration

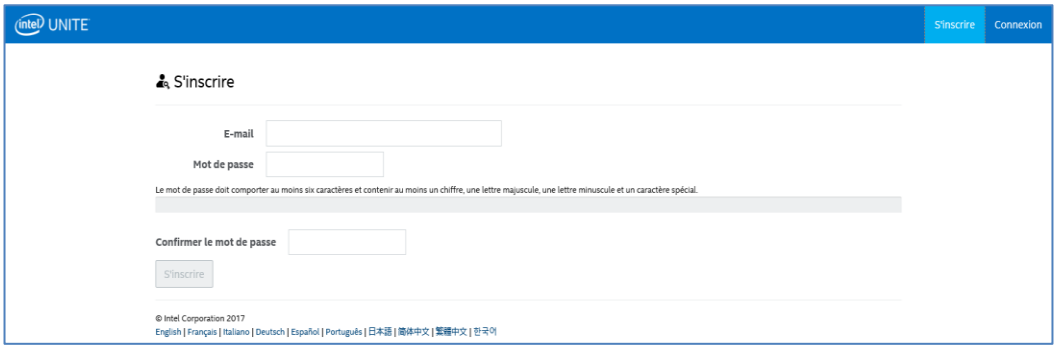
La page d'accueil s'affiche lorsque vous vous connectez au portail administrateur. Pour accéder à la page d'accueil, vous devez vous connecter avec le compte par défaut créé à l'étape d'installation ou à l'aide des identifiants de votre compte.



8.1.1 Enregistrement d'un compte

Pour enregistrer un compte, déconnectez-vous du portail administrateur.

- Cliquez sur le lien **S'inscrire** situé en haut à droite de la barre de navigation.
- Renseignez l'adresse e-mail et le mot de passe requis dans le formulaire, puis cliquez sur **S'inscrire**.



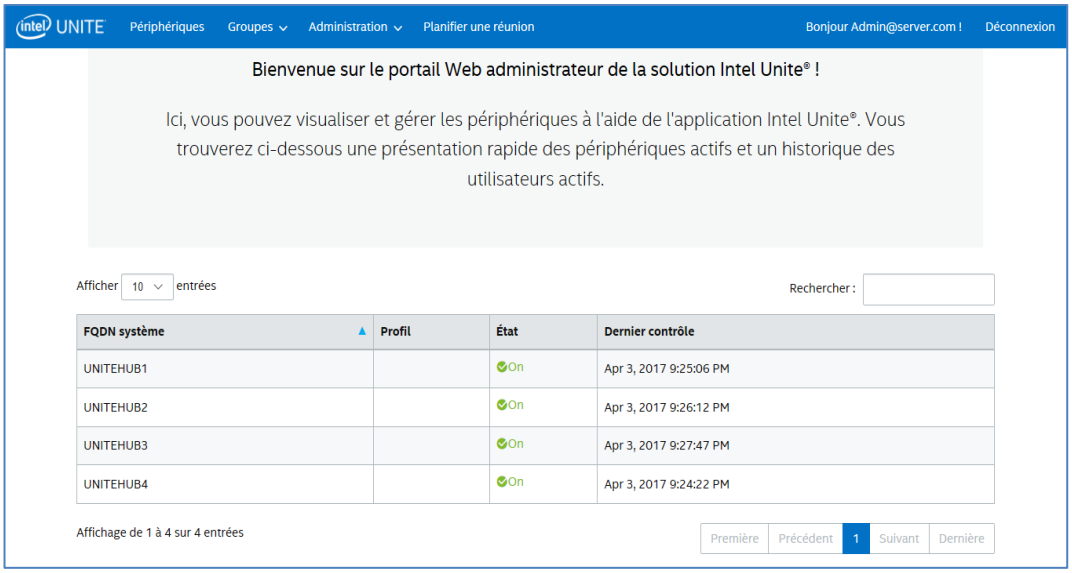
- Vous pouvez également ajouter ou enregistrer des utilisateurs depuis l'onglet Administration lorsque vous êtes connecté au portail administrateur.

8.1.2 Connexion à l'aide d'un compte existant

Vous pouvez vous connecter avec un compte enregistré ou utiliser le compte par défaut créé lors de l'installation. Pour rappel, ce compte dispose d'un accès complet au portail administrateur, mais vous serez invité à en modifier le mot de passe afin d'assurer l'accès réservé au portail.

8.2 Page d'accueil du portail administrateur

Cette page d'accueil affiche un message de bienvenue et fournit un aperçu de tous les systèmes actifs (clients et concentrateurs) connectés au serveur. Le tableau affiche le nom de chaque **système**, le **profil** associé à chaque système, l'état **ON** ou **OFF** et l'heure et la date du **dernier contrôle**.



Les données du tableau peuvent être filtrées à l'aide de la barre de recherche et de différents mots clés. Chaque mot clé sera recherché dans les colonnes. Vous pouvez sélectionner le nombre de données que vous souhaitez afficher dans cette fenêtre en cliquant sur Afficher <nombre d'>entrées. Vous pouvez afficher 10, 25, 50 ou jusqu'à 100 entrées.

8.2.1 Barre de navigation

La barre de navigation vous dirigera vers les différentes rubriques du portail Web et vous indiquera qui est l'utilisateur actuellement connecté ou indiquera la mention **S'inscrire** si aucun utilisateur n'est connecté.

Les pages principales et secondaires du portail Web sont les suivantes :

- **Périphériques**
- **Groupes**
  - Groupe de périphériques
  - Profils
- **Administration**
  - Propriétés du serveur
  - Utilisateurs
  - Rôles
  - Modérateurs
  - Code PIN réservé
  - Télémétrie
- **Planifier une réunion**

Pour en savoir plus sur ces pages, consultez la section consacrée à chaque sujet de ce chapitre sur le portail administrateur.

8.2.2 Nomenclature des icônes et des liens

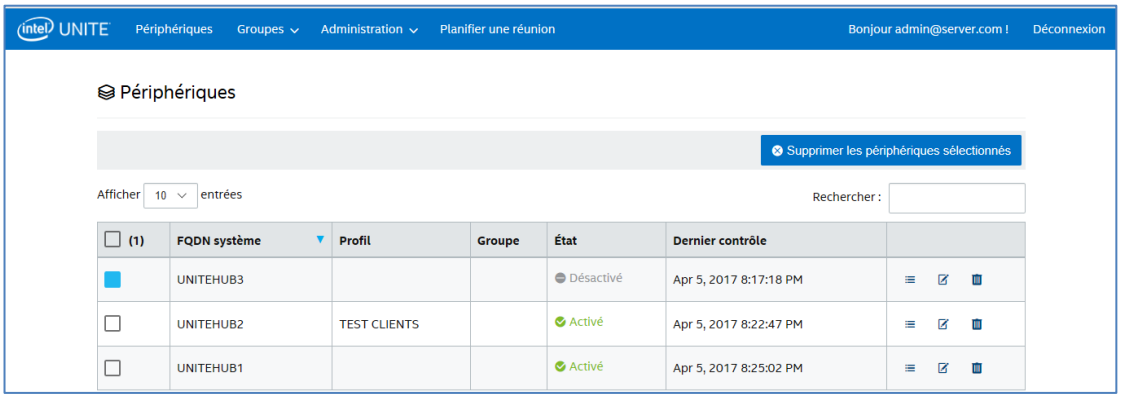
Les icônes ou liens suivants sont utilisés sur le portail administrateur :

	Modifier
	Voir détails
	Afficher les périphériques
	Supprimer
	Boîte de dialogue contenant des informations sur une valeur spécifique

Lorsque vous passez le pointeur de la souris sur l'icône, des informations sur l'élément en question s'affichent.

8.3 Page Périphériques

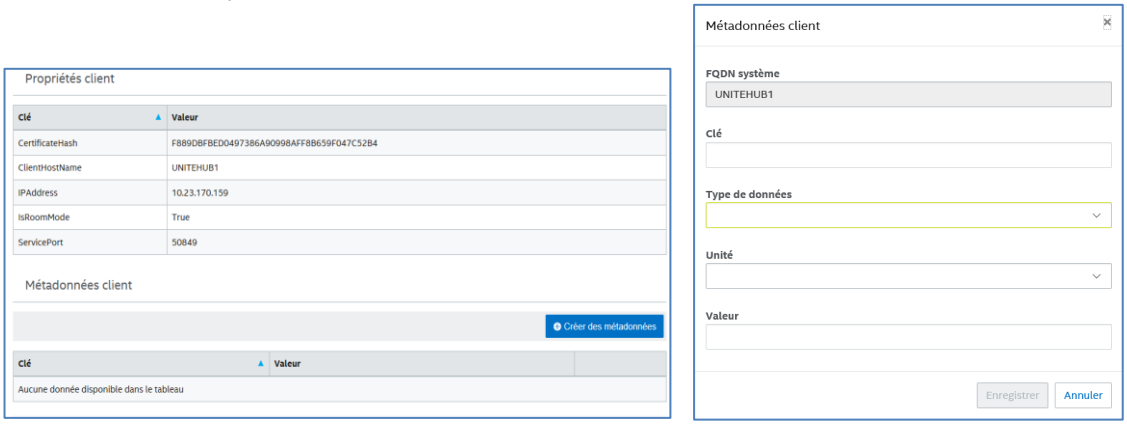
La page Périphériques affiche l'ensemble des périphériques présents dans la base de données. Vous pouvez sélectionner un appareil spécifique et l'**afficher**, le **modifier**, le **mettre à jour** ou le **supprimer** si vous le souhaitez.



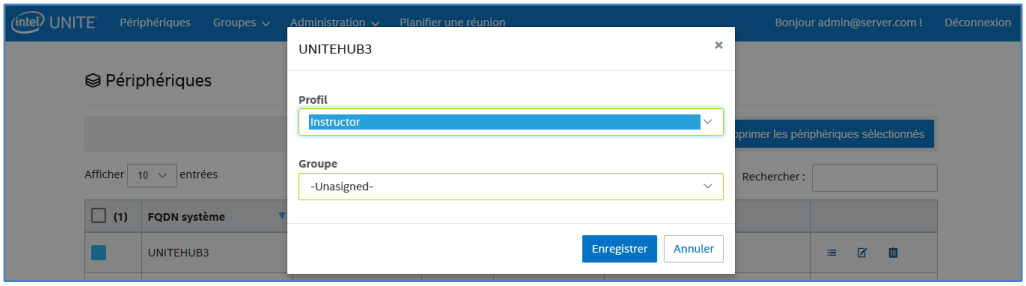
Sur la page **Périphériques** figurent les éléments suivants :

- **FQDN système** : nom de domaine complet du client ou du concentrateur.
- **Profil** : dispose des paramètres de configuration appliqués à l'appareil.
- **Groupe** : le nom du groupe dans lequel se trouve un appareil.
- **État**: indique si l'appareil est actif (activé, vert) ou inactif (désactivé, gris).
- **Dernier contrôle** : dernière connexion du périphérique au serveur.
- **Détails** : en cliquant sur le lien **Voir détails**, la fenêtre **Propriétés client** s'affiche. Y figurent les propriétés et les métadonnées du système. Certaines des clés sous **Propriétés client** sont les suivantes :
    - CertificateHash
    - ClientHostName
    - IPAddress
    - IsRoomMode
    - SevicePort

Pour en savoir plus sur les valeurs valides de chaque clé, consultez la section Configuration de profil. Vous y trouverez des informations détaillées sur les clés et les valeurs correspondantes.



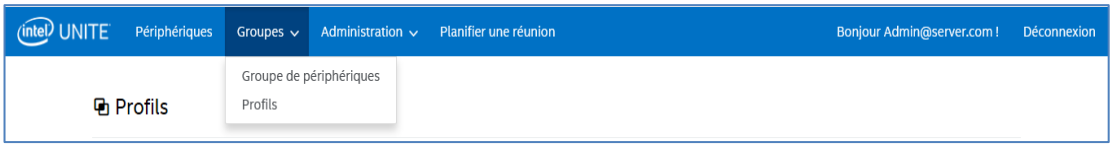
Lien **Modifier** : cliquer sur le lien Modifier vous permet de modifier le profil de l'appareil et d'attribuer un groupe donné à l'appareil.



Lien **Supprimer** : cliquer sur le lien Supprimer supprime l'appareil du portail administrateur. Un message de confirmation indiquant que l'appareil a été supprimé s'affiche. Vous pouvez également sélectionner un ou plusieurs appareils dans la colonne de gauche et cliquer sur le bouton **Supprimer les périphériques sélectionnés**.

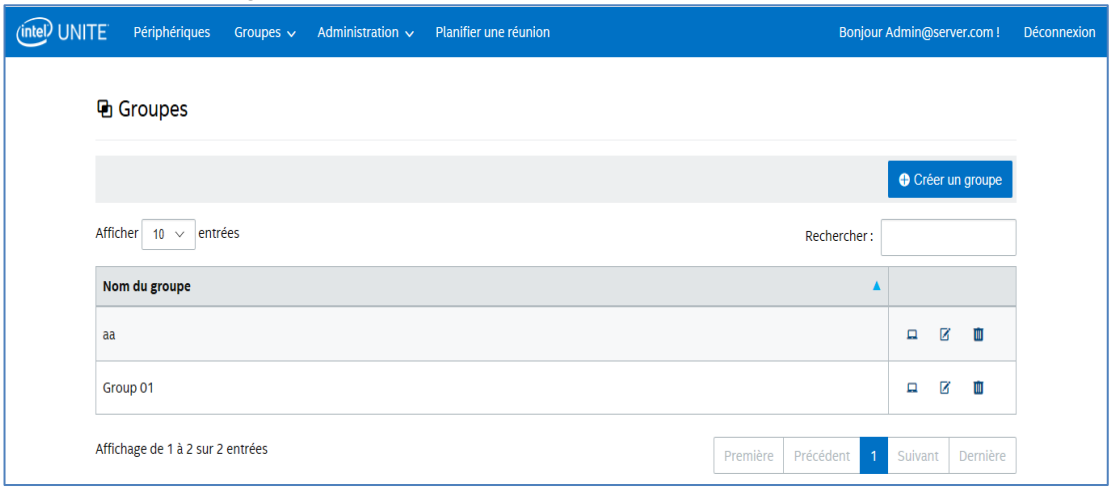
8.4 Page Groupes

Le menu propose deux options pour la page **Groupes** : **Groupe de périphériques** et **Profils**.



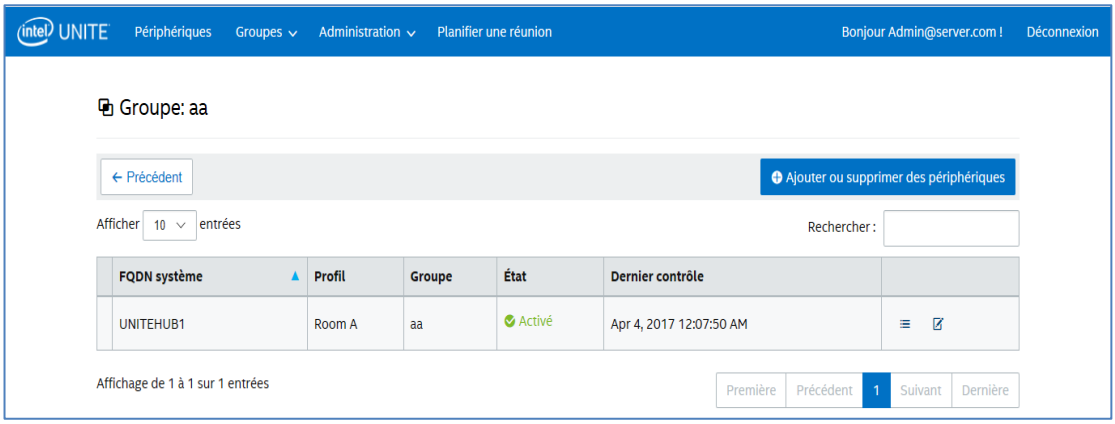
8.4.1 Groupes > Groupe de périphériques

Groupe de périphériques permet de regrouper les appareils à des fins de surveillance, de fonctionnalités ou de commodité. Il est possible d'assigner des appareils avec le même profil ou avec des profils différents à un groupe. Cette page permet de créer, d'afficher, de modifier et de supprimer les groupes et les données de chaque groupe. Vous pouvez créer un nouveau groupe en cliquant sur **Créer un groupe** et en fournissant le nom du groupe.



Une fois le groupe créé, vous pouvez :

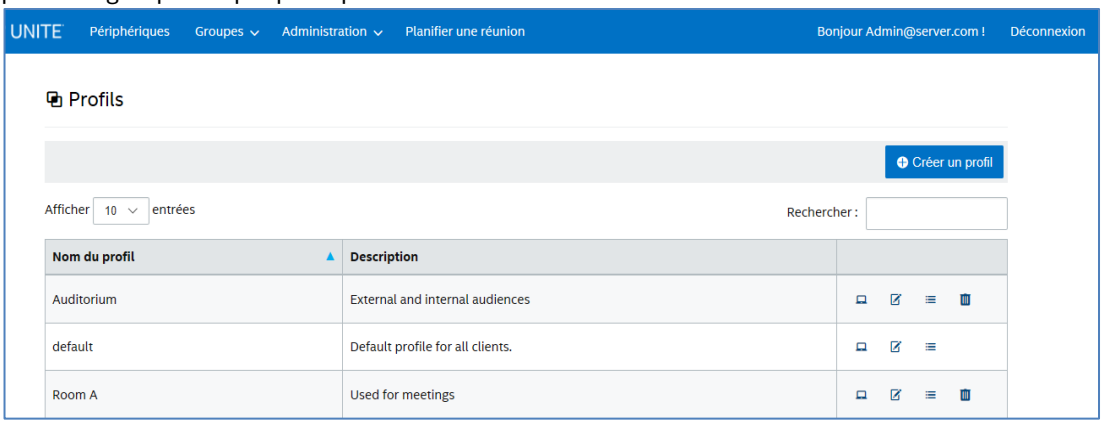
- Cliquer sur le lien **Afficher les périphériques** pour ajouter des appareils au groupe sélectionné ou les supprimer du groupe sélectionné. Vous pouvez également cliquer sur le lien **Détails** dans la colonne de droite pour afficher les propriétés et les métadonnées de chaque système du groupe.



- Cliquer sur le lien **Modifier** pour mettre à jour ou modifier le **nom du groupe**.
- Si vous apportez des modifications, cliquez sur **Enregistrer** pour sauvegarder les changements.

8.4.2 Groupes > Profils

Cette page vous permet de créer, de voir, de supprimer et de modifier les profils. La fonction et la présentation de cette page sont similaires à celles de la page **Groupes de périphériques**, sauf qu'elle contient des profils. La différence entre les **profils** et les **groupes** est que les profils contiennent les options de configuration des périphériques. Les périphériques ne peuvent appartenir qu'à un seul profil mais à plusieurs groupes de périphériques.



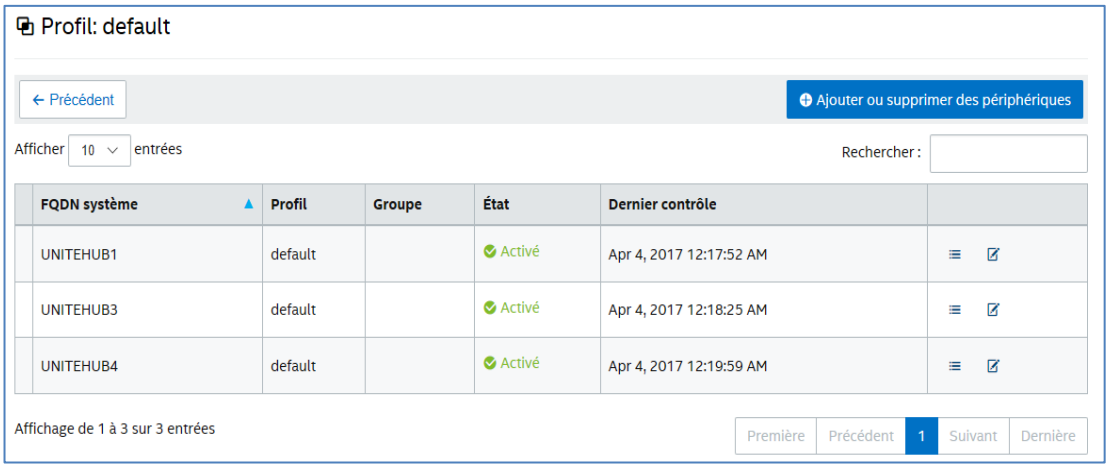
La page **Profils** affiche le **nom du profil** et la **description** de chaque profil sur le serveur. Les profils sont appliqués à tous les appareils se connectant au serveur d'entreprise. Le profil **default** ne peut pas être supprimé du portail administrateur.

En cliquant sur le lien **Afficher les périphériques**, vous pourrez voir les systèmes attribués au profil sélectionné.
En cliquant sur le lien **Modifier**, vous pouvez mettre à jour le nom du profil et sa description.

En cliquant sur le lien **Afficher les détails** d'un profil particulier, vous pouvez accéder et modifier les paramètres des clés et des valeurs du profil par défaut ou nouvellement créé. Une liste des clés et de leurs valeurs ainsi que le lien **Modifier** s'affichent afin de vous permettre de faire les mises à jour et les modifications personnalisées de votre choix. Consultez la section *Configuration de profil* pour obtenir des informations détaillées sur les clés et les valeurs correspondantes.

8.4.2.1 Profil par défaut

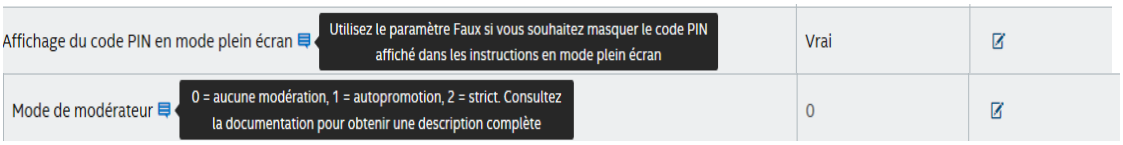
Le profil **par défaut** ne peut pas être supprimé du portail administrateur. Vous pouvez créer d'autres profils, en sachant que le profil par défaut ne peut pas être supprimé.



Valeurs et clés **par défaut** :

Clé	Valeur
Autoriser le transfert de fichiers	Faux
Assistance au streaming audio et vidéo	Vrai
Modifier le code PIN pendant la réunion	Vrai
Désactiver l'affichage à distance	Faux
Taille du code PIN affiché	48
Afficher la transparence du code PIN	100
Extensions de fichiers bloquées	
Taille maximale des fichiers	2147483647
Mode plein écran	Vrai
Couleur d'arrière-plan du mode plein écran	
Image étirée en arrière-plan en mode plein écran	Faux
URL d'arrière-plan du mode plein écran	
Instructions du mode plein écran	{pin}
Couleur du code PIN en mode plein écran	
Affichage du code PIN en mode plein écran	Vrai
Couleur du texte en mode plein écran	
Police du texte en mode plein écran	
Concentrateur : verrouiller le clavier	Faux
Concentrateur : afficher l'horloge	Vrai
Mode de modérateur	0

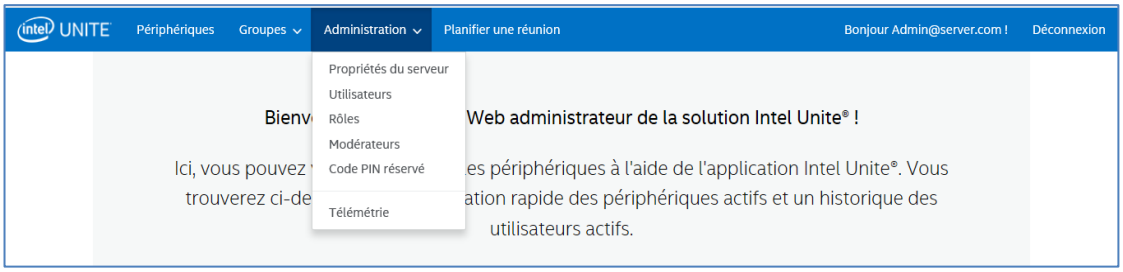
Veuillez noter qu'une boîte de dialogue se trouve en regard de chaque clé. Lorsque vous passez le pointeur sur la boîte de dialogue, les valeurs de chaque clé et/ou des informations sur les clés s'affichent, afin que vous disposiez des renseignements nécessaires pour modifier les clés. Vous trouverez deux exemples ci-dessous :



Vous pouvez également vous référer au tableau figurant à la section Configuration de profil pour consulter des informations détaillées sur les clés et les valeurs correspondantes.

8.5 Page Administration

La page Administration se divise en plusieurs sous-sections :

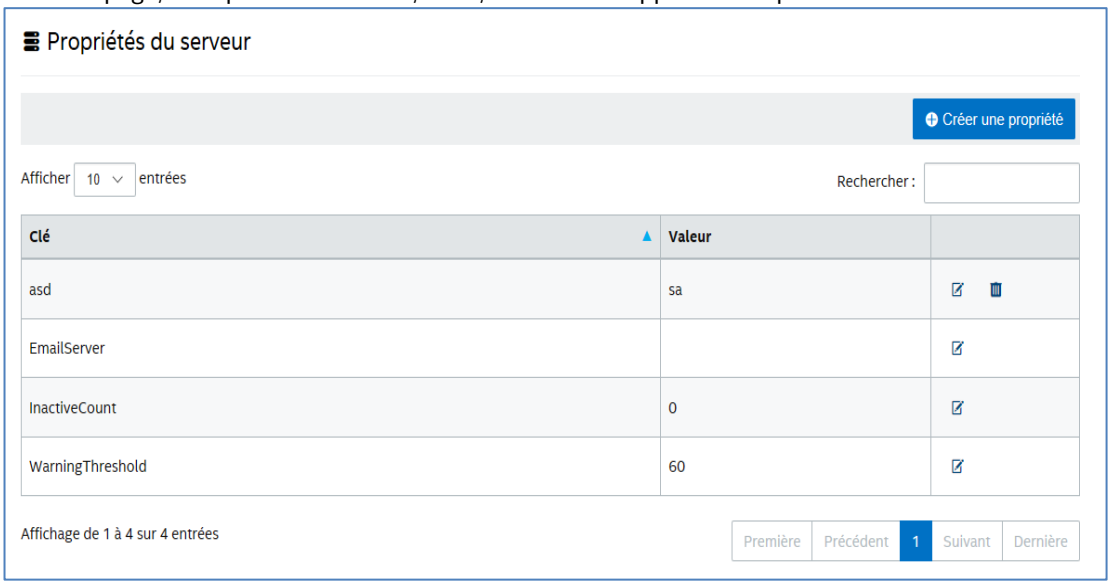


- **Propriétés du serveur** : il s'agit de l'interface utilisée pour consulter et modifier les valeurs et clés de serveur.
- **Utilisateurs** : vous pouvez ajouter, supprimer ou modifier manuellement n'importe quel compte sur cette page.
- **Rôles** : vous permet de créer de nouveaux rôles, de mettre à jour les rôles existants, d'attribuer des rôles à des utilisateurs et de modifier les autorisations des utilisateurs.
- **Modérateurs** : cette fonctionnalité permet aux utilisateurs de prendre le contrôle d'une réunion en répartissant les fonctionnalités par rôle. Dans cette section, vous pouvez facilement ajouter ou supprimer des modérateurs.
- **Code PIN réservé** : cette fonctionnalité permet aux administrateurs informatiques d'attribuer des codes PIN à certaines salles. Les codes PIN peuvent être générés automatiquement ou être définis manuellement par le service informatique, en fonction des besoins de la session ou de l'emplacement de la salle.
- **Télémétrie** : pour afficher les données de télémétrie, le plug-in de télémétrie de la solution Intel Unite® doit être installé. Le plug-in de télémétrie permet aux administrateurs informatiques de recueillir des données d'utilisation concernant l'application Intel Unite® et les appareils clients connectés à chaque concentrateur.

Pour plus d'informations sur ces sous-pages, consultez les rubriques ci-dessous.

8.5.1 Administration > Propriétés du serveur

Sur cette page, vous pouvez consulter, créer, modifier et supprimer des paires de valeurs de clé de serveur.



Les clés utilisées par le portail administrateur sont les suivantes :

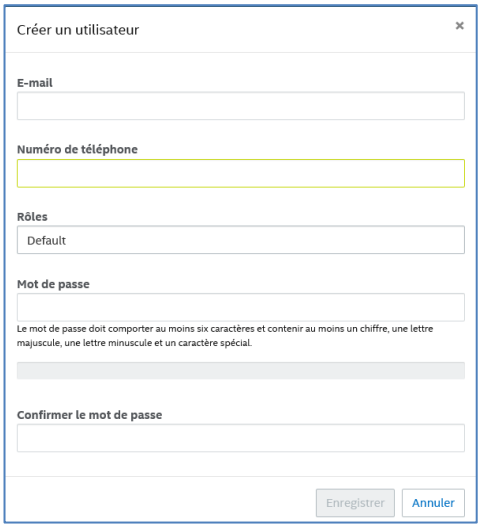
- **EmailServer** : il s'agit de l'adresse e-mail à laquelle le serveur envoie les notifications.
- **InactiveCount :** utilisé par l'outil de surveillance de l'état de l'application Intel Unite®, qui envoie un e-mail aux utilisateurs auxquels le rôle Notifications a été attribué.
- **WarningThreshold** : utilisé pour déterminer le seuil auquel un appareil est considéré comme inactif, en minutes. La valeur par défaut est 60 minutes.

En cliquant sur le lien **Modifier**, vous pouvez mettre à jour les clés en fonction de vos besoins.

8.5.2 Administration > Utilisateurs

La page **Utilisateurs** affiche une liste de tous les utilisateurs enregistrés sur le portail administrateur, indique si leur compte a été bloqué et indique leur rôle. Vous pouvez également mettre à jour ces informations en cliquant sur le lien **Modifier**.

Vous pouvez ajouter un nouvel utilisateur en cliquant sur **Créer un utilisateur** et en fournissant un e-mail, un numéro de téléphone et un mot de passe. Lors de la création d'un utilisateur, vous pouvez également lui attribuer un rôle donné ou conserver les paramètres par défaut. Pour donner des droits d'accès aux nouveaux utilisateurs, vous pouvez définir des rôles et les attribuer aux utilisateurs.

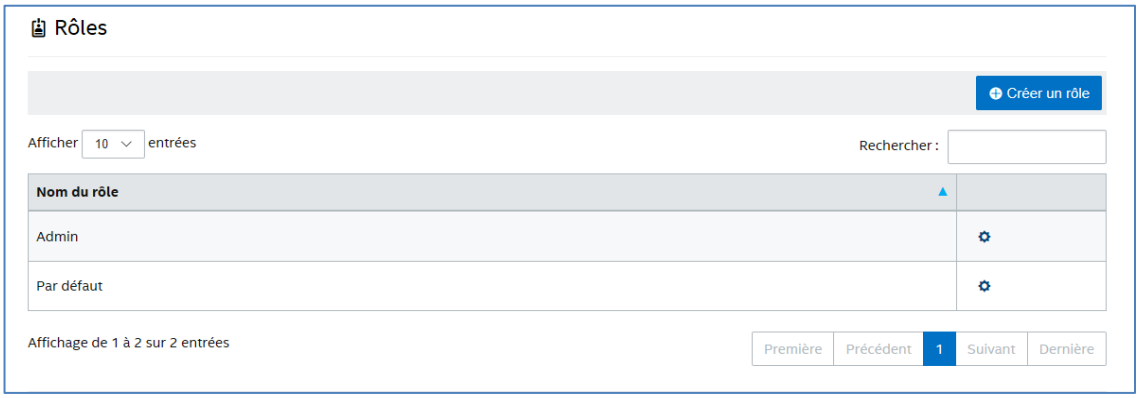


Sur cette même page, si vous cliquez sur le rôle (**Par défaut** ou **Admin**), la page **Rôles** s'ouvre. Consultez la section suivante pour en savoir plus sur les **Rôles**.

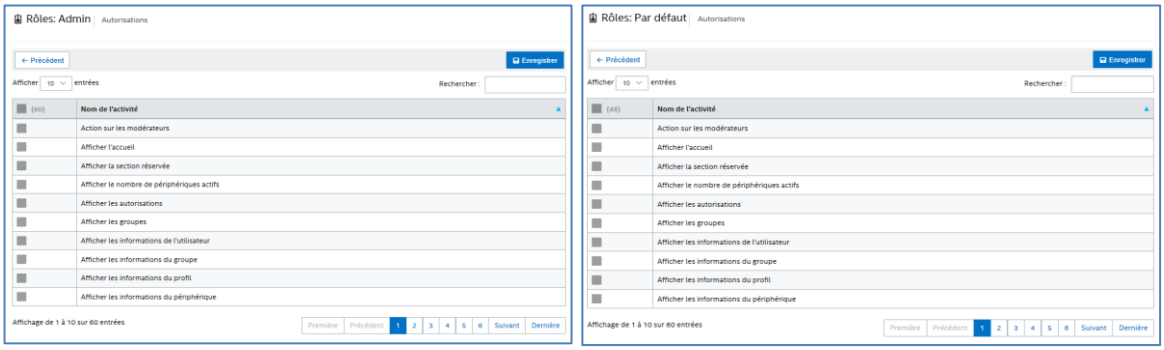
REMARQUE concernant le compte par défaut : un e-mail de vérification ne sera pas envoyé automatiquement lors de l'ajout d'un nouveau compte d'utilisateur via la connexion au compte par défaut admin@server.com. Pour vérifier manuellement l'adresse e-mail, connectez-vous au nouveau compte, cliquez sur « Bonjour <votre nom d'utilisateur> ! » en haut à droite de la barre de navigation, puis cliquez sur le bouton « **Envoyer un e-mail de vérification** » au bas de la page. Avant de le faire, vous devez modifier les paramètres de messagerie de votre serveur dans le fichier XML web.config. Voir la rubrique Paramètres du serveur de messagerie électronique.

8.5.3 Administration > Rôles

Cette page affiche les rôles actuellement définis, à savoir **Admin** et **Par défaut**. Vous pouvez ajouter de nouveaux rôles et modifier des rôles existants. Les rôles seuls ne régulent pas l'accès au portail. Les actions sur le portail (par ex. la création d'un utilisateur) sont restreintes aux rôles, qui sont associés à des ensembles d'utilisateurs.



Pour afficher les activités et les autorisations associées à chaque rôle, cliquez sur l'icône en forme d'engrenage dans la colonne de droite. La fenêtre **Autorisations** s'affiche. Les activités attribuées peuvent être personnalisées pour permettre à un ensemble de rôles de les réaliser.



Pour ajouter un nouveau rôle, cliquez sur le bouton **Créer un rôle** et modifiez le nom du rôle. Puis, sur la page **Rôles**, cliquez sur l'icône en forme d'engrenage et sélectionnez les activités que vous souhaitez associer à ce rôle. Cette option vous permet d'ajouter ou de supprimer des autorisations.
Sachez que plusieurs rôles peuvent être attribués aux utilisateurs.

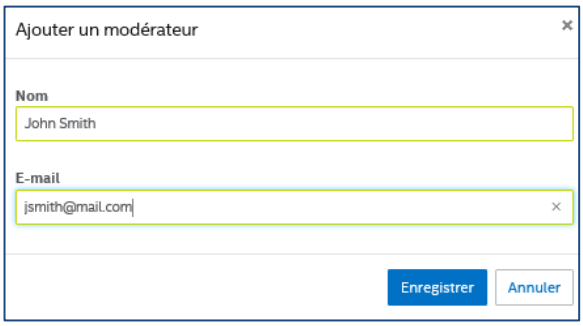
8.5.4 Administration> Modérateurs

Cette page affiche les utilisateurs qui ont le rôle de modérateur. Pour définir un utilisateur comme modérateur, vous devez suivre plusieurs étapes.

Vous pouvez ajouter un modérateur de deux façons : en cliquant sur **Ajouter un modérateur** et en renseignant les informations demandées ou en important un fichier CSV comportant les noms et les adresses e-mails des utilisateurs que vous souhaitez ajouter à la liste en cliquant sur **Importer les modérateurs depuis le fichier CSV**. Si vous importez un fichier CSV où figurent les noms des modérateurs, veuillez à ce qu'il respecte le format suivant : **Nom,E-mail,Action** ou cliquez sur le **fichier d'exemple** pour consulter le format valide.

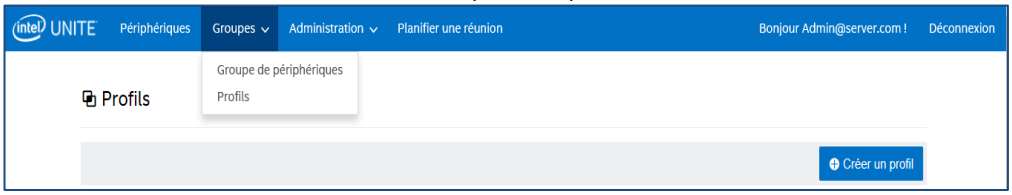
Exemple : John Smith,jsmith@aaa.com,Ajouter
Sandra Leon,sleon@bbb.com,Supprimer

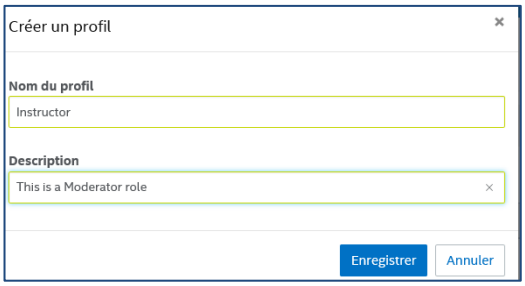
Cliquez sur **Ajouter un modérateur** pour saisir manuellement le **nom** et l'adresse **e-mail** du modérateur, puis cliquez sur **Enregistrer**.



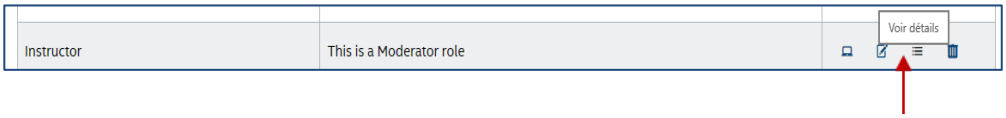
Le mode de la fonction Modérateur doit être défini sur le profil du concentrateur, afin que vous disposiez d'un environnement mixte sur vos systèmes. Effectuez ensuite les étapes suivantes :

- Accédez à la page **Groupes** et sélectionnez **Profils**, puis cliquez sur **Créer un profil**. Lorsque la fenêtre s'ouvre, saisissez le nom et la description du profil souhaité.

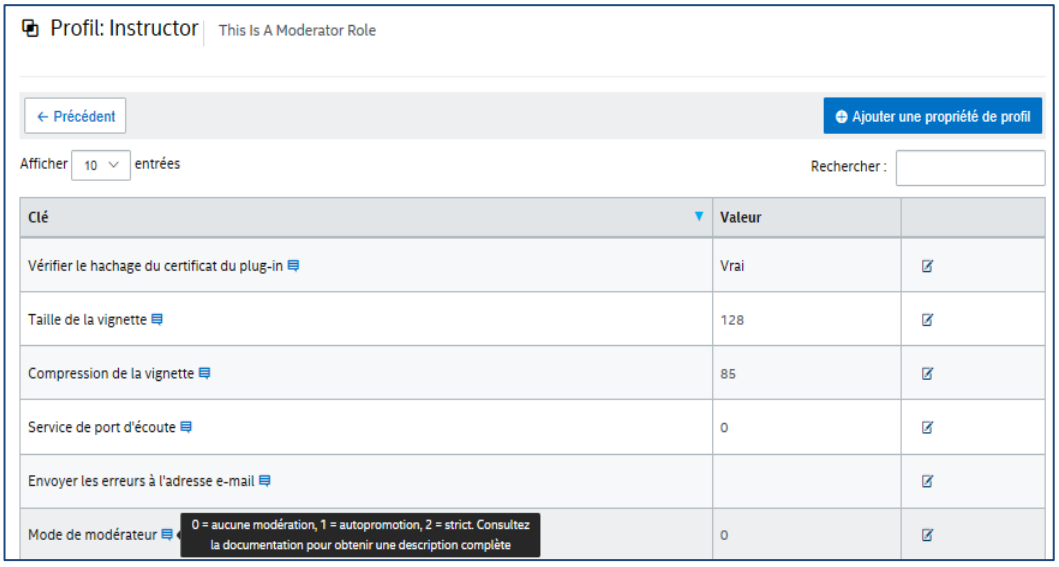




- Une fois le profil créé, repérez-le dans la liste. Dans la colonne de droite en regard du profil, cliquez sur Voir détails.



- Dans la colonne **Clé**, repérez la clé **Mode de modérateur** et saisissez la **valeur** souhaitée pour le mode que vous souhaitez appliquer au profil. Consultez les valeurs valides ci-dessous :



Description et valeurs concernant les modérateurs :

0- **Non géré** : mode par défaut. Aucun modérateur pendant la réunion/la session, tous les participants ont les mêmes droits d'affichage et d'animation. Les versions du logiciel Intel Unite® antérieures à la version v3.1 utilisaient ce mode.

1- **Auto-promu** : la réunion/la session n'est pas gérée tant que personne n'assume le rôle du modérateur. Dans ce cas de figure, seul le modérateur peut attribuer le rôle de modérateur à un autre participant. Le modérateur peut également décider qui anime pendant la session.

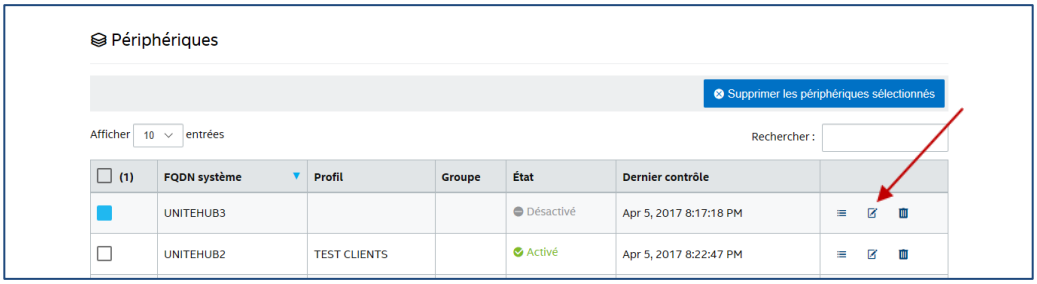
2- **Strict** : la réunion/session est gérée uniquement par le modérateur désigné. Lorsqu'un modérateur rejoint la session, il endosse automatiquement ce rôle.

Remarques :

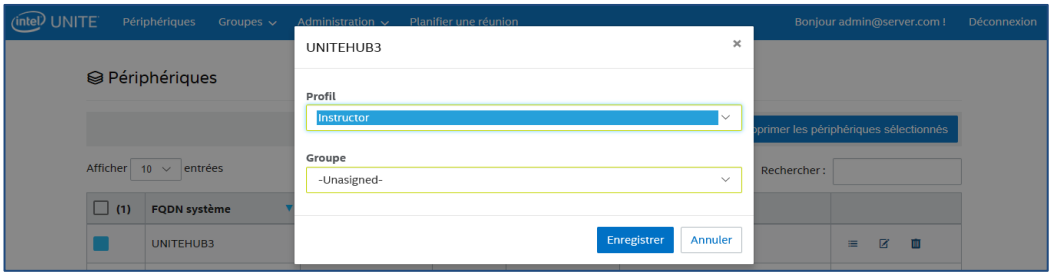
a. La liste des modérateurs est gérée par l'administrateur informatique depuis le portail administrateur. Les modérateurs sont authentifiés à l'aide d'une clé associée à leur adresse e-mail. Lorsqu'un utilisateur est désigné en tant que modérateur, le portail administrateur lui envoie un e-mail contenant un URI : lorsque l'utilisateur clique dessus, le jeton de modérateur s'installe sur le client. Les utilisateurs doivent suivre cette procédure une fois uniquement pour chaque système.

b. L'administrateur informatique peut révoquer les droits de modération en supprimant le jeton de l'utilisateur du portail administrateur.
c. Pour envoyer des e-mails d'enregistrement aux modérateurs, le service informatique doit configurer un relais SMTP, afin que la fonctionnalité soit disponible. Consultez la section **Configuration des modérateurs** pour en savoir plus.
d. Si vous n'avez pas de relais SMTP et que vous devez gérer manuellement l'URI envoyé par e-mail, suivez la procédure ci-après :
Accédez à l'onglet **Administration** et sélectionnez **Propriétés du serveur**. Cliquez sur le lien **Modifier** en regard de **EmailServer** et saisissez le nom du relais SMTP, par exemple : smtp.exemple.com:22
Vous pouvez uniquement configurer un relais SMTP qui n'exige pas une authentification. Il est également possible d'obtenir et d'installer manuellement le jeton de modérateur d'un utilisateur. Pour plus d'informations, consultez la section **Installation manuelle du jeton en mode strict**.

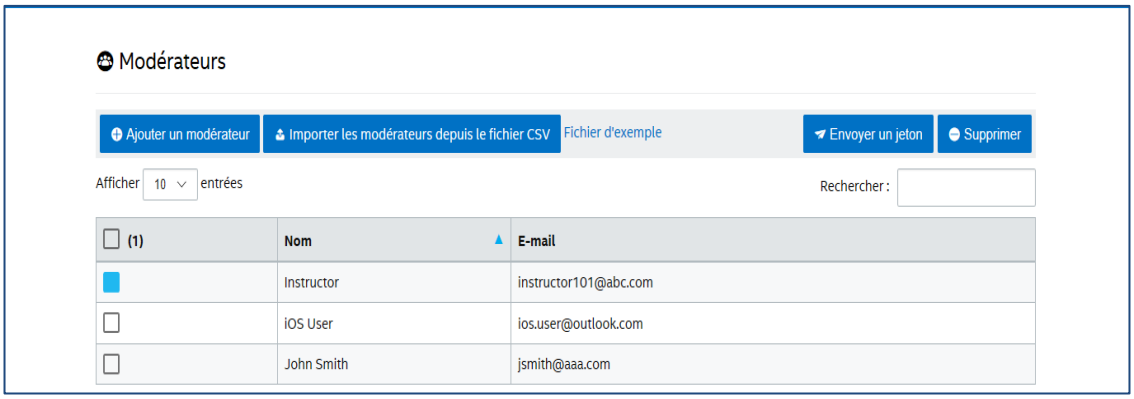
- Pour activer le profil du modérateur sur un concentrateur donné, accédez à la page **Périphériques**, sélectionnez le concentrateur à configurer dans la liste et cliquez sur le lien **Modifier** se trouvant dans la colonne de droite.



- Lorsque la fenêtre s'ouvre, sélectionnez le profil créé pour le modérateur dans la section Profil, ainsi que le groupe auquel il appartient (le cas échéant) et cliquez sur **Enregistrer**.



Vous pouvez supprimer les modérateurs de votre choix de la liste créée en les sélectionnant (case bleue) et en cliquant sur **Supprimer**. Pour envoyer à un modérateur une URL permettant de rejoindre une réunion/session, cliquez sur son nom, puis sur **Envoyer un jeton**.



8.5.4.1 Installation manuelle du jeton en mode strict

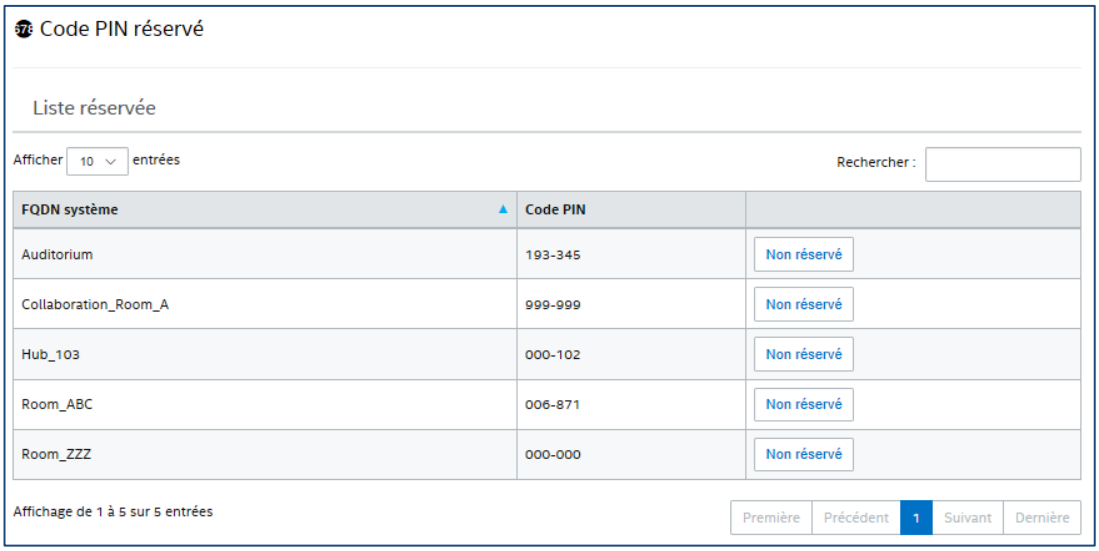
Si vous ne disposez pas d'un relais SMTP, il est possible d'obtenir et d'installer manuellement le jeton de modérateur d'un utilisateur défini comme modérateur. Pour ce faire, Microsoft SQL Server Management Studio doit être installé.
Pour obtenir le jeton :

- Ajoutez un modérateur.
- Ouvrez Microsoft SQL Server Management Studio et connectez-vous au serveur de base de données au moyen des identifiants admin utilisés lors de l'installation du serveur d'entreprise.
- Développez « Bases de données », puis « UniteServer », puis « Tableaux ».
- Avec le bouton droit de la souris, cliquez sur « dbo.Moderators », puis sur « Select Top 1000 ».
- Dans la liste des résultats, localisez le nom d'utilisateur qui correspond à celui ajouté à l'étape précédente.
- Faites un clic droit et copiez le jeton dans le presse-papier.
- Ouvrez le bloc-notes et créez l'URI : intelunite://localhost/SetModerationToken?Token=<collez le jeton copié à l'étape précédente>.
- Ouvrez Intel Unite®.
- Sur les appareils Windows : ouvrez l'Explorateur, effectuez un copier-coller de l'URI complet et appuyez sur Entrée.
- Sur les appareils Mac : ouvrez Safari, effectuez un copier-coller de l'URI complet et appuyez sur Entrée.

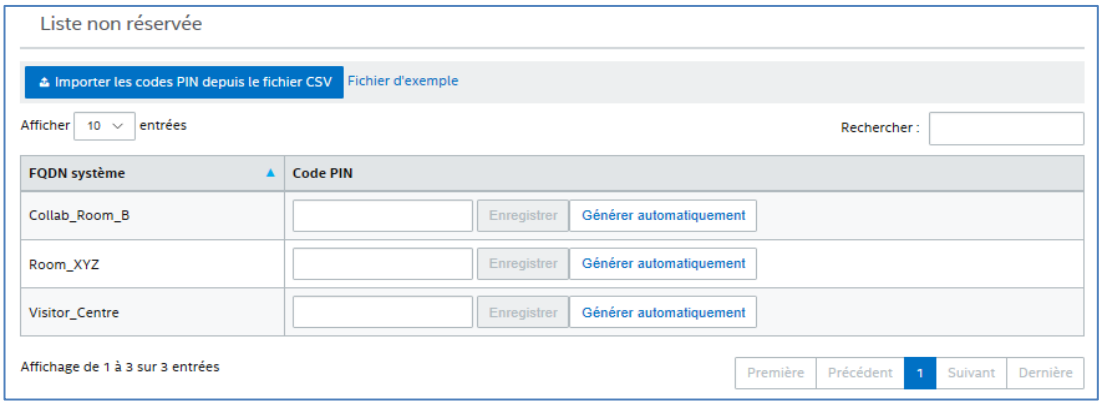
8.5.5 Administration> Code PIN réservé

Cette page affiche deux sections, à savoir la liste **Réservée** et la liste **Non réservée** des systèmes dont le code PIN affiché pendant la réunion/session est statique ou non. L'administrateur informatique peut associer des systèmes à des salles données pour lesquelles les utilisateurs devront saisir le même code PIN pendant la réunion/session ou devront saisir un code PIN changeant (valeur par défaut).

- **Liste réservée :** il s'agit de la liste des réservations que le service informatique a déjà configurées. Vous pouvez les annuler en cliquant sur **Non réservé**.



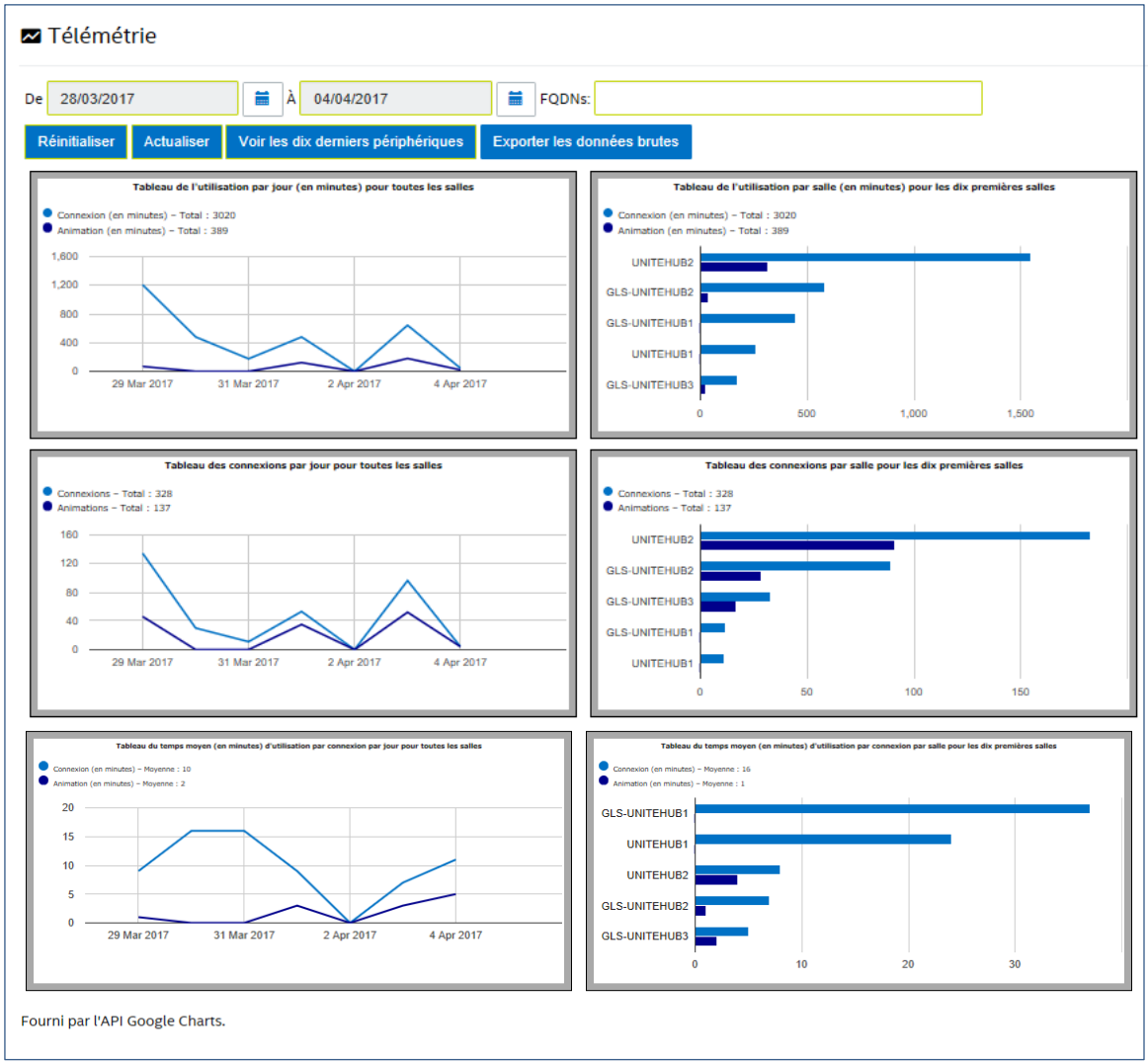
- **Liste non réservée :** il s'agit de la liste des systèmes qui n'ont pas de réservations de codes PIN statiques. Il est possible d'ajouter manuellement des codes PIN, de les générer automatiquement ou de les importer à partir d'un fichier CSV.



Lorsque vous attribuez des codes PIN, cliquez sur **Enregistrer** pour conserver les valeurs définies.

8.5.6 Administration> Télémétrie

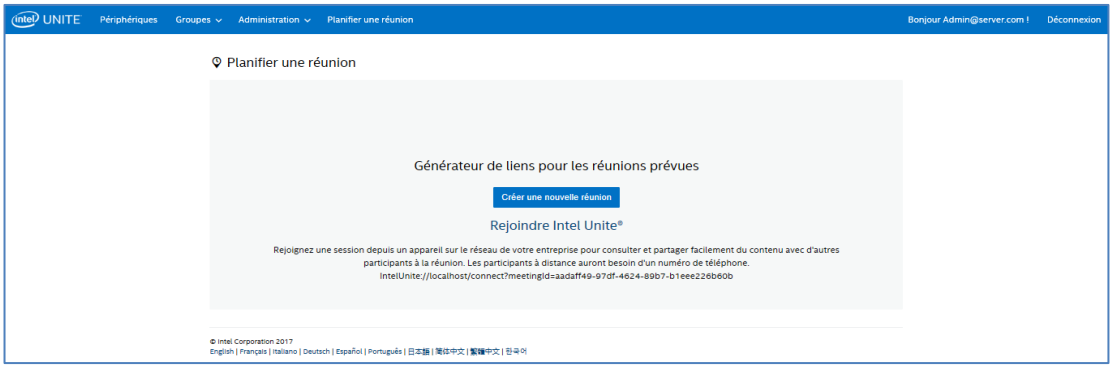
Cette page affiche les données de télémétrie recueillies par le portail administrateur. Pour consulter ces données, le plug-in de télémétrie de la solution Intel Unite® doit être installé. Le plug-in de télémétrie permet aux administrateurs informatiques de recueillir des données d'utilisation concernant l'application Intel Unite® et les appareils clients connectés à chaque concentrateur. Les administrateurs informatiques auront accès à des informations comme le nombre de connexions dans chaque salle, le nombre de connexions par jour, la durée moyenne par connexion, etc. Veuillez consulter le **Guide relatif au plug-in Intel Unite® de télémétrie** pour obtenir des informations détaillées et déployer le plug-in sur votre système.



8.6 Page Planifier une réunion

La page Planifier une réunion permet de créer une URL de réunion pour les participants à une réunion/session qui ne peuvent pas installer ou utiliser le plug-in Intel Unite® pour Microsoft Office existant. Tous les participants peuvent voir cette page.

Pour créer une URL, puis l'envoyer aux utilisateurs qui participeront à la réunion/session, il suffit de cliquer sur le bouton **Créer une nouvelle réunion**.



8.7 Autres options de configuration du portail administrateur

8.7.1 Configuration de profil

Les profils peuvent être configurés en accédant à **Groupes** > **Profils** et en cliquant sur **Détails** sur le profil du portail administrateur. Cela affiche les paramètres de configuration sous la forme d'une paire de valeurs clé. Vous pouvez modifier les valeurs afin de personnaliser l'application et l'expérience de l'espace de réunion/de la session. Par exemple, l'image d'arrière-plan de l'affichage du concentrateur, la taille du code PIN, la couleur de la police et le contenu sont des paramètres qui peuvent être utilisés.
Après avoir personnalisé les valeurs d'un profil, attribuer des périphériques au profil pour appliquer les paramètres de configuration du profil. Pour appliquer le profil à des appareils, cliquez sur le lien **Afficher les périphériques**, puis sur **Actualiser la liste des périphériques**. La liste des périphériques s'affiche. Cochez la case en regard du périphérique de votre choix pour appliquer les paramètres de configuration.

Le tableau suivant présente les **clés** disponibles, leur description, le type de données et les valeurs par défaut des clés.

Clé	Description	Type de données	Valeurs par défaut
Autoriser le transfert de fichiers	Indicateur qui active ou désactive la possibilité, pour un concentrateur ou un client, de transférer un fichier.	Booléen	Faux
Assistance au streaming audio et vidéo	Indicateur permettant aux utilisateurs de Windows de partager leur ordinateur de bureau en A/V (1080p à 20-30 ips).	Booléen	Vrai
Modifier le code PIN pendant la réunion	Permet de bloquer le code PIN d'une réunion/session. Le code PIN restera le même jusqu'à ce que tous les utilisateurs se déconnectent. Vrai : autorise le changement du code PIN pendant la session. Faux : bloque le code PIN pendant la	Booléen	Vrai

	session.		
Désactiver l'affichage à distance	Désactive la fonction d'affichage à distance dans certaines salles. Lorsque cette option est utilisée, si un participant essaie d'afficher du contenu à l'aide de la fonction d'affichage à distance, une image indiquant que la fonction n'est pas disponible s'affiche. Vrai : désactive l'affichage à distance. Faux : autorise l'affichage à distance.	Booléen	Faux
Taille du code PIN affiché	Taille en pixels. Cette valeur est la taille en pixels du code PIN à l'écran (des valeurs plus grandes facilitent la lecture du code PIN d'un bout à l'autre de la salle).	Nombre entier	48
Afficher la transparence du code PIN	Contrôle la transparence alpha du code PIN qui s'affiche sur le moniteur. 100 : entièrement visible. 1 à 99 : le code PIN et le cadre autour de lui sont visibles. L'opacité change en fonction de la valeur utilisée. 0 : le code PIN est transparent.	Nombre entier	100
Extensions de fichiers bloquées, affichées en tant qu'Extensions de fichiers bloquées	Liste séparée par des virgules des extensions de fichiers bloquées (p. ex. exe, bin, msi).	Chaîne	Vierge
Taille maximale de fichier affichée en tant que Taille maximale de fichier	Taille de fichier maximale pour les transferts.	Nombre entier	2147483647 octets (plage valide : 0 à 2147483647)
Mode plein écran	Active ou désactive le plein écran du concentrateur. Faux : code PIN dans le coin supérieur droit uniquement Vrai : code PIN dans le coin supérieur droit et arrière-plan en grand écran	Booléen	Vrai
Couleur d'arrière-plan du mode plein écran	Couleur d'arrière-plan utilisée sur le concentrateur. Couleurs HTML (couleurs hexadécimales). Exemples de valeurs valides (valeurs RVB, format #000000) : Rouge : #FF0000 Jaune : #FFFF00 Vert : #00FF00 Bleu clair : #00FFFF Bleu foncé : #0000FF Noir : #000000 Blanc : #FFFFFF Gris : #808080	Chaîne	Vierge (s'affiche en noir)
Image étirée en arrière-plan en mode plein écran	Indicateur permettant de faire en sorte que l'image d'arrière-plan soit appliquée à l'ensemble de l'écran.	Booléen	Faux
URL d'arrière-plan du mode plein écran	Configure le fond d'écran du concentrateur sur l'URL ou l'image (jpg/png) spécifiée. Configurez la	Chaîne	Vierge

	valeur sur « Vrai » si vous souhaitez activer cette fonctionnalité. Exemple : http://monserveur.com/background.jpg		
Instructions du mode plein écran	Instructions textuelles à afficher sur le concentrateur. Possibilité d'utiliser {pin} et {hôte} en remplacement URL de téléchargement du client. Cet élément s'affiche en mode plein écran.	Chaîne	{pin}
Couleur du code PIN en mode plein écran	Couleur du code PIN qui s'affiche.	Chaîne	Vierge (s'affiche en blanc)
Affichage du PIN en mode plein écran	Affiche les instructions. Configurez la valeur sur « Vrai » si vous souhaitez activer cette fonctionnalité.	Booléen	Vrai
Couleur du texte en mode plein écran	Couleur du texte affiché sur le concentrateur.	Chaîne	Vierge (s'affiche en blanc)
Police du texte en mode plein écran	Nom de la police des instructions.	Chaîne	Vierge
Concentrateur : verrouiller le clavier	Verrouillage de Ctrl-Esc, Alt-Tab, la barre d'icônes, les clés Windows et Alt-F4 dans le concentrateur. S'il est configuré sur Vrai, le verrouillage du concentrateur est activé. Peut être remplacé par un mot de passe configuré dans les clés de registre Machine (valeur REG KEY).	Booléen	Faux
Concentrateur : afficher l'horloge	Affiche l'horloge dans le coin inférieur droit.	Booléen	Vrai
Mode de modérateur	Définit le mode de modérateur lors des réunions/sessions. Utilisez les valeurs suivantes : 0 : aucune modération 1 : autopromotion 2 : strict	Nombre entier	0
Envoyer les erreurs à l'adresse e-mail	Définit l'adresse e-mail à laquelle le concentrateur enverra les messages d'erreur.	Chaîne	Vierge (s'affiche en blanc)
Service de port d'écoute	Un port pour permettre au concentrateur d'écouter les connexions entrantes.	Nombre entier	0 (0 : port auto-attribué)
Compression de la vignette	Permet d'ajuster le rapport de compression du partage de contenu non-AV. Pourcentage de compression à appliquer à une portion modifiée de l'affichage (vignette) transmise sur le réseau. (Les valeurs élevées sont gourmandes en bande passante.)	Nombre entier	85 (plage valide : 5 à 100)
Taille de la vignette	Permet d'ajuster la taille des vignettes pour le partage de contenu non-AV. Taille des vignettes après	Nombre entier	128 (plage valide : 32 à 512)

	division de l'écran en plusieurs blocs. Taille de chaque vignette en pixels.		
Vérifier le hachage du certificat du plug-in	Les plug-ins doivent être vérifiés. Vrai : vérifier le hachage du certificat Faux : ne pas vérifier le hachage du certificat	Booléen	Vrai

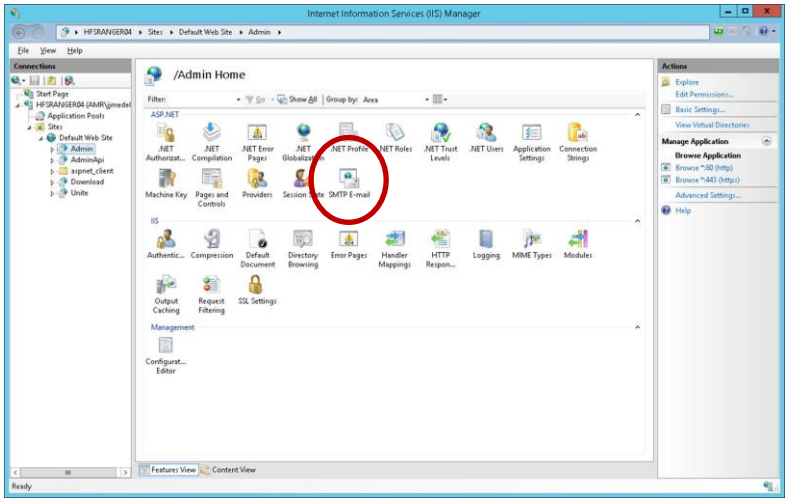
8.7.2 Intervalle d'actualisation du code PIN

L'intervalle d'actualisation par défaut du code PIN est de 5 minutes, c'est-à-dire que le PIN qui s'affiche sur le concentrateur change toutes les 5 minutes. Il peut être modifié par incréments d'une minute de 2 à 60 minutes en modifiant le fichier **web.config** à la racine du répertoire virtuel du site du service Web. L'accès se fait depuis le gestionnaire des services IIS. Pour localiser le fichier, accédez au répertoire Intel Unite\PinServer. Par défaut, il est installé au chemin C:\Program Files (x86)\Intel\Intel Unite\PinServer. Modifiez la valeur sous <add key="**PinExpireTimeInMinutes**" value="5"></add> pour obtenir l'intervalle d'actualisation souhaité.

8.7.3 Paramètres du serveur de messagerie électronique

Le portail administrateur défini le serveur SMTP dans le fichier XML web.config créé lors de l'installation de l'application Intel Unite® sur le serveur. En fonction de l'emplacement où est configuré le serveur SMTP, le paramètre **mailSettings** doit être modifié dans le fichier XML web.config de sorte que l'« hôte » pointe vers votre serveur SMTP. (Par défaut, le fichier XML Web.config est sous C:\Program Files (x86)\Intel\Intel Unite\PinServer).
Assurez-vous que le serveur de messagerie SMTP est bien configuré sous le Gestionnaire des services Internet (IIS) et que le paramètre fonctionne bien avec l'application pendant la préinstallation du serveur d'entreprise.
Les paramètres du fichier sont les suivants :

```
<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 Service d'alerte et de surveillance

Le serveur d'entreprise propose des services d'alerte et de surveillance. Il s'agit d'un service à activer qui se configure dans le portail administrateur.
Un périphérique configuré pour recevoir des alertes est surveillé. S'il ne se connecte pas avant le seuil d'avertissement, un e-mail est envoyé aux utilisateurs spécifiés.
Pour autoriser la réception d'e-mails relatifs aux périphériques inactifs, assurez-vous que le rôle **Notifications** a été attribué à l'utilisateur depuis le portail administrateur. Pour activer la surveillance d'un périphérique, ajoutez la clé **EnableReporting** à ses métadonnées et définissez la valeur sur **Vrai**.
Le seuil d'avertissement peut être configuré depuis la commande **Administration** > **Propriétés du serveur** et est défini sur 60 minutes par défaut.
InactiveCount : si un utilisateur souhaite recevoir immédiatement un e-mail lors de la vérification suivante, il doit configurer un seuil inférieur.
L'adresse e-mail (smtp from) et le serveur de messagerie (host) doivent être indiqués dans le fichier **clocktower.exe.config**, qui se trouve sous : /productfiles/release/clocktower.exe.config. (Par défaut, l'emplacement du fichier clocktower.exe xml config est C:\Program Files (x86)\Intel\Intel Unite\ClockTower)

Les paramètres du fichier sont les suivants :

```
<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>
```

8.7.5 Configuration des modérateurs

Pour configurer des modérateurs, vous devez d'abord configurer un relais SMTP afin que la fonctionnalité soit disponible. Sans cela, les modérateurs ne pourront pas recevoir les jetons nécessaires et un message d'erreur s'affichera lors des tentatives d'envoi des jetons.
Localisez le fichier web.conf se trouvant sous C:\Program Files (x86)\Intel\Intel Unite\WebApi et ajoutez ce qui suit :

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

Insérez ces éléments dans le fichier entre les balises <system.net></system.net>.

Remarque : « smtp.example.com » doit être modifié de manière à faire apparaître votre serveur de messagerie (il convient de remplacer « example » par le nom de votre serveur).

9 Contrôles de sécurité pour système d'exploitation et ordinateur

9.1.1 Normes de sécurité minimales (MSS)

Il est recommandé que tous les périphériques exécutant l'application Intel Unite® respectent les normes de sécurité minimales par défaut de votre entreprise, de disposer d'un agent d'application de correctifs, d'un anti-virus, d'IPS, d'IDS et d'autres mesures de contrôle selon la spécification MSS (McAfee suite contre les logiciels malveillants, IPS, IDS testé pour sa compatibilité).

9.1.2 Renforcement machine

L'interface UEFI (Machine Unified Extensible Firmware Interface) peut être verrouillée pour lancer le chargeur d'amorçage Windows uniquement (de manière à ce que le lancement à partir d'une clé USB ou d'un DVD ne fonctionnera pas), la fonctionnalité Bit de verrouillage doit être activée, ainsi que la technologie d'exécution fiabilisée Intel® et les paramètres verrouillés par mot de passe.

Renforcement du SE Windows : tout d'abord, le système s'exécute sans droits d'utilisateur élevés. Il est également recommandé de supprimer les logiciels inutilisés du système d'exploitation, notamment les logiciels pré-installés inutiles et les composants Windows (services PowerShell, service d'impression et de numérisation de document, service de localisation Windows, services XPS).

Verrouillage du sous-système d'interface graphique : comme le système utilise un écran non tactile, il s'avère plus difficile de sortir du sous-système d'interface graphique rien qu'avec le clavier et la souris. Pour empêcher les pirates informatiques d'ajouter un périphérique HID (clavier/souris USB), il est recommandé de faire un blocage par programmation à l'aide des commandes **Alt+Tab**, **Ctrl+Maj+Échap** et de la barre des **icônes**.

9.1.3 Autres commandes de sécurité

Il est recommandé de verrouiller le compte utilisateur de chaque compte machine dans Active Directory. Si le déploiement comprend un grand nombre d'unités, les comptes utilisateur peuvent être verrouillés, comme lorsque l'on verrouille un étage particulier d'un immeuble, en cas d'incendie par exemple.

Propriété des machines : Il est recommandé que chaque machine ait un propriétaire identifié. Dans le cas où une machine se déconnecte sur une longue période, son propriétaire identifié en sera averti.
En plus des mécanismes de sécurité fournis par la plate-forme Intel® vPro™ et le logiciel Intel Unite® lui-même, il est recommandé de renforcer la sécurité du système d'exploitation Microsoft* Windows conformément aux recommandations de Microsoft pour la sécurisation renforcée des machines. Pour en savoir plus, consultez le gestionnaire* de configuration de sécurité (SCM) de Microsoft au lien suivant : https://technet.microsoft.com/fr-fr/solutionaccelerators/cc835245.aspx
Remarque : les informations dans ce lien contiennent un outil de renforcement de la sécurité basé sur un assistant, y compris les meilleures méthodes connues et la documentation correspondante.

10 Maintenance

Votre entreprise et votre administrateur informatique décideront de la mise en place d'un programme de maintenance régulier. Il est recommandé de procéder aux tâches de maintenance suivantes :

10.1 Redémarrage quotidien

Il est recommandé de procéder à un redémarrage quotidien des concentrateurs (de préférence pendant la nuit) et, avant ce redémarrage, d'effectuer des tâches de maintenance telles que la suppression des fichiers temporaires du cache et le lancement de la procédure d'application des correctifs standard.

10.2 Stratégie d'application de correctifs

Si possible, exécutez votre procédure d'application de correctifs standard en mode sans assistance (sans invite de l'interface utilisateur), de préférence avant le redémarrage quotidien.

10.3 Rapports

Collectez les indicateurs de temps d'activité des machines et établissez un rapport selon les besoins de votre entreprise.

10.4 Surveillance

Utilisez un système de suivi des performances s'appuyant sur les pulsations des machines et réalisez une analyse du temps d'activité en arrière-plan selon les besoins.

10.4.1 Surveillance en arrière-plan :

Utilisez des outils standard de surveillance de serveur virtuel pour générer et envoyer des alertes au support technique de deuxième niveau.

11 Solution Intel Unite® pour macOS

11.1 Introduction

Le logiciel Intel Unite® pour macOS se présente sous la forme d'un package applicatif principal et peut comporter des valeurs informatiques de préférences spécifiques. Ainsi, l'application prend en charge différents déploiements courants, des logiciels et des techniques de gestion Mac généraux à l'installation manuelle et au paramétrage des préférences.

11.2 Flux de connexion général

Par défaut, l'application utilise la découverte automatique DNS (p. ex. l'enregistrement de service DNS) pour déterminer le serveur d'entreprise auquel se connecter. Le flux de travail général est le suivant :

- (Facultatif) Serveur d'entreprise défini dans les préférences.
- Découverte automatique des domaines suivants :
  - _uniteservice._tcp
  - _uniteservice._tcp.votreSousDomaine.votreDomaine.votreTLD
    i. Exemple : _uniteservice._tcp.corp.acme.com
  - _uniteservice._tcp.votreDomaine.votreTLD
    i. Exemple : _uniteservice._tcp.acme.com
  - Tentative de connexion au protocole HTTPS, puis au protocole HTTP en cas d'échec
- uniteservice.votreDomaine.votreTLD

11.3 Valeurs des préférences

L'équipe informatique peut modifier et personnaliser l'application Intel Unite® afin qu'elle réponde aux exigences d'infrastructure ou de sécurité de l'entreprise en définissant les paramètres suivants dans com.intel.Intel-Unite.plist, qui se trouve dans le dossier ~/Bibliothèque/Préférences de chaque utilisateur :

- **Définition d'un serveur d'entreprise par défaut**
  defaults write com.intel.Intel-Unite EnterpriseServer monServeur.monDomaine.monTLD

- **Définition d'une clé publique de serveur d'entreprise pour l'épinglage du certificat**
  defaults write com.intel.Intel-Unite EnterpriseServerPublicKey "clé publique"

- **Forcer un client à autoriser uniquement les certificats de serveur autorisés**
  defaults write com.intel.Intel-Unite ClientOnlyAllowsTrustedCertificates -bool true

- **Forcer un client à se connecter en mode autonome**
  defaults write com.intel.Intel-Unite Standalone -bool true

Chacun de ces paramètres peut être défini ou modifié manuellement en ouvrant le terminal macOS (/Applications/Utilitaires) et en saisissant la commande suivie d'un retour à la ligne. Les détails et les informations sur chaque commande sont les suivants :

- **Définition d'un serveur d'entreprise par défaut**
  La définition d'un serveur d'entreprise par défaut interrompra le processus de découverte automatique. Si vos clients Mac se trouvent uniquement sur votre propre réseau, ce paramètre peut être utile pour épingler l'application Intel Unite® à un serveur d'entreprise particulier pour des raisons de sécurité ou à des fins de dépannage.

- **Définition d'une clé publique de serveur d'entreprise pour l'épinglage du certificat**
  Pour épingler l'application client à votre serveur d'entreprise, que la découverte automatique soit utilisée ou non, vous pouvez définir la clé publique sur chaque client. Pour obtenir cette valeur :
  - Ouvrez Safari sur un Mac de votre réseau d'entreprise.
  - Accédez à l'adresse HTTPS de votre serveur d'entreprise.
  - Cliquez sur l'icône en forme de cadenas de la barre d'adresses.
  - Cliquez sur le bouton **Afficher le certificat** de la fiche de certificat.
  - Cliquez sur le triangle **Détails** pour développer les données.
  - Parcourez les données du certificat jusqu'à ce que vous trouviez le champ **Informations de la clé publique** > **Clé publique**.
  - Cliquez sur le champ de données, qui commence par « 256 octets : »
  - Le champ de données se développe.
  - Sélectionnez toutes les données du champ avec la souris ou à l'aide de la commande CMD+A.
  - Copiez les données dans le presse-papier en sélectionnant **Copier** dans le menu contextuel ou en utilisant la commande **CMD+C**.
  - Dans la commande par défaut, remplacez la **clé publique** par les données du presse-papier. Remarque : vous devrez mettre les données entre guillemets.

  Tout comme avec la définition d'un serveur d'entreprise par défaut, l'activation de cette option rendra difficile la connexion des utilisateurs à la solution Intel Unite® installée par d'autres partenaires/à d'autres emplacements.

- **Forcer un client à autoriser uniquement les certificats de serveur autorisés**
  Outre définir un serveur d'entreprise spécifique ou épingler la clé publique du certificat, vous pouvez également indiquer à l'application Intel Unite® de n'autoriser que les connexions aux serveurs/certificats entièrement autorisés par votre chaîne d'approbation de certificat. Vous devez vous assurer que le certificat de votre serveur d'entreprise est lié à un serveur racine public, comme défini par Apple dans la chaîne de clé, ou que vous avez installé votre propre certificat racine de serveur et tout autre certificat intermédiaire nécessaire sur chaque client.

- **Forcer un client à se connecter en mode autonome**
  La définition de ce mode modifie le flux de connexion : celui-ci effectue une découverte automatique UDP du concentrateur qui a généré un PIN dans un environnement, sans serveur d'entreprise. Dans ce cas de figure, le système basé sur le processeur Intel Core vPro agit en tant qu'hôte principal et est utile dans l'environnement d'une PME, lorsqu'il n'y a pas de service informatique pour installer l'infrastructure du serveur d'entreprise. Ce mode fonctionnera uniquement sur les systèmes se trouvant sur le même sous-réseau que celui où les paquets UDP ne sont pas bloqués.

11.4 Méthodologies courantes de distribution

Si vous utilisez la découverte automatique, la distribution peut être aussi simple que de déposer l'application Intel Unite® dans le dossier Applications. Dans des environnements plus complexes ou dans les environnements qui nécessitent des paramètres de sécurité supplémentaires, vous pouvez définir des préférences spécifiques en plus de la distribution du package d'application. Il existe différents moyens de le faire. Voici les plus courants :

- Script Bash
  - ➢ Vous pouvez définir vos paramètres préférés dans un script Bash qui peut être distribué aux utilisateurs avec le package d'application.
- Personnalisation du package d'installation à l'aide de PackageMaker
  - ➢ Vous pouvez définir vos paramètres préférés à l'aide d'un script de survol en amont ou en aval.
- Personnalisation de l'installation à l'aide d'Apple Remote Desktop

- À l'aide d'Apple Remote Desktop, vous pouvez installer le package d'application Intel Unite® et définir les paramètres préférés depuis le menu **Envoyer la commande UNIX...**.

- Installation personnalisée depuis un logiciel de gestion Mac pour entreprise
  - Vous pouvez créer une installation personnalisée tirée ou poussée à l'aide des solutions d'entreprise courantes de gestion Mac.
    - Casper / Bushel
    - Puppet
    - Munki
    - Chef
    - Etc.

12 Dépannage

12.1 Impossible d'accéder à la page du portail administrateur après l'installation d'Intel Unite® sur le serveur

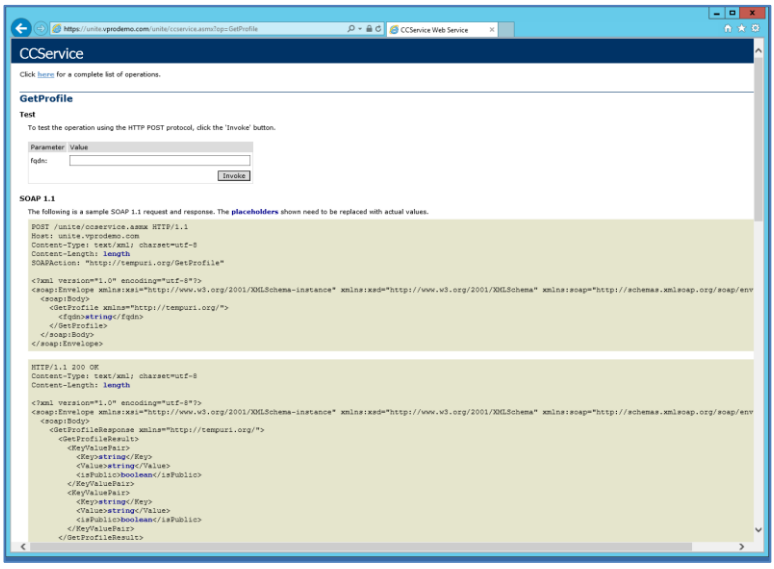
Solution de contournement/Solution : assurez-vous que les rôles et les fonctionnalités nécessaires pour le serveur Web ont été ajoutés au serveur.

- Ajoutez des rôles et des fonctionnalités au serveur utilisant le gestionnaire de serveur.
    - Rôles du serveur : serveur Web
        - Ajoutez les outils de gestion.
    - Ajoutez les fonctionnalités .NET Framework 3.5.
    - Ajoutez les fonctionnalités .NET Framework 4.
        - ASP .NET
            - Services WCF
            - Activation HTTP
        - Rôles du serveur Web :
            - Serveur Web, fonctionnalités HTTP courantes et document par défaut.

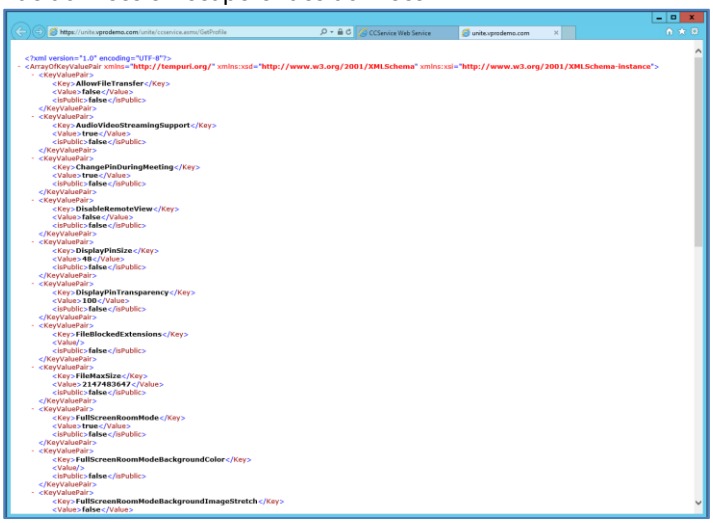
12.2 Accès au portail administrateur impossible

Si, lorsque vous accédez au portail administrateur, une page d'erreur s'affiche indiquant un problème avec une balise xml spécifique dans Web.config, supprimez la balise de Web.config dans le niveau supérieur du répertoire virtuel du portail (accessible à partir de la console de gestion IIS).

- Pour vérifier que l'installation du service Web a réussi, suivez ce lien :
  https://<votrenomdeserveur>/unite/ccservice.asmx
    - Sélectionnez **GetProfile**.
    - Saisissez **test** dans le champ de **valeur**, puis cliquez sur Invoke (Appeler).



- Vérifiez que vous pouvez afficher un profil par défaut dans le fichier XML, comme illustré ci-dessous. Cela indique que le service PIN peut accéder à la base de données et récupérer des données.



12.3 Erreur lors du lancement du concentrateur de l'application

Une fenêtre contextuelle fournit le code de l'erreur. En fonction du code, la nature de l'erreur peut être déterminée.

12.3.1 La vérification de la plate-forme a échoué avec le code d'erreur 333333

Cette erreur indique que le concentrateur a fait une vérification de plate-forme, mais que le certificat de signature de code n'a pas pu être validé. Cela est généralement dû à l'absence de certificat racine à jour sur le système d'exploitation, ce qui empêche le certificat de signature de code public d'Intel Unite® d'être validé.
Assurez-vous que le système est connecté à Internet, ouvrez un navigateur et rendez-vous sur le site https://www.microsoft.com (afin de forcer le système à mettre à jour les certificats racines).

12.3.2 La vérification de la plate-forme a échoué avec le code d'erreur 666666

Cette erreur indique que la plate-forme n'est pas compatible avec l'application Intel Unite®. Contactez le fournisseur OEM pour vous assurer que vous disposez d'une plate-forme compatible avec l'application.

12.4 Le concentrateur n'obtient pas de PIN de la part du serveur PIN. Affichage de tiret de défilement.

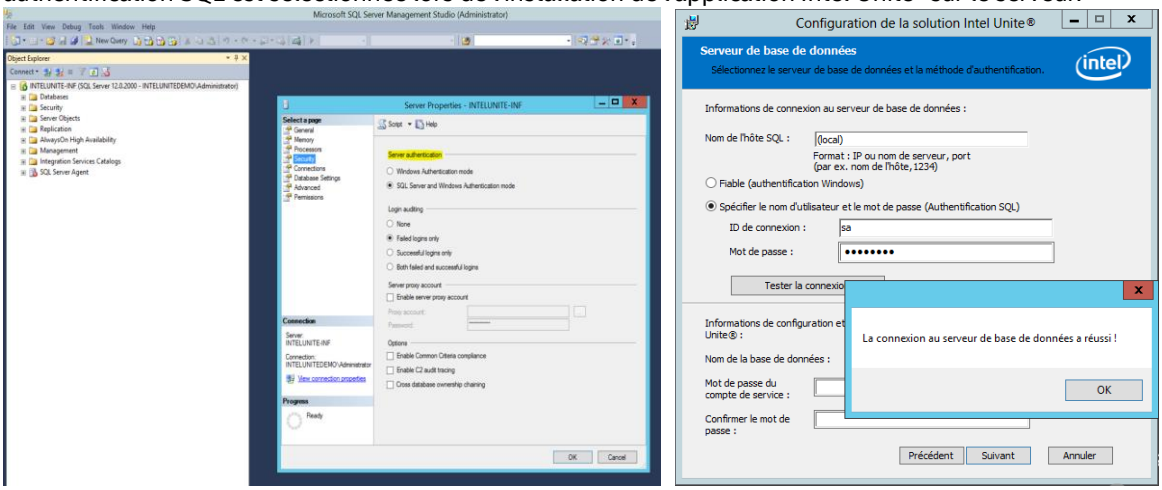
Lancez l'application Intel Unite® sur le concentrateur avec un commutateur de débogage : naviguez jusqu'au dossier où l'application est enregistrée à l'aide d'une invite de commande et exécutez la commande de débogage suivante : **IntelUnite.exe** /debug
Une fenêtre de débogage s'ouvre et affiche les informations de connexion. Certaines erreurs courantes et leurs solutions de contournement sont répertoriées ci-dessous. Si les informations de débogage contiennent l'une de ces erreurs, suivez les solutions/solutions de contournement indiquées pour résoudre le problème et générer un code PIN sur le concentrateur.

12.4.1 Traitement de la requête par le serveur impossible ; échec de la connexion pour l'utilisateur UniteServiceUser

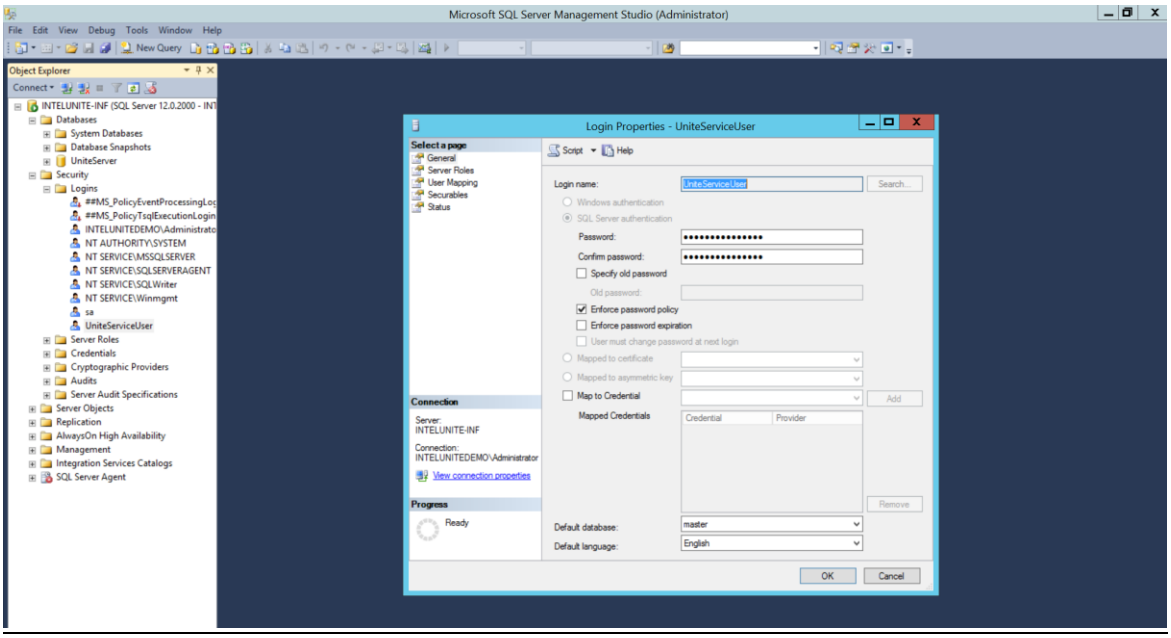
Cela peut se produire si les identifiants de connexion SQL sont incorrects ou si le mot de passe de la base de données est corrompu, car un utilisateur essaie d'installer le serveur d'entreprise plusieurs fois.

Solution de contournement/Solution :

Vérifiez les modes d'authentification utilisés pendant l'installation de MS SQL. Pour modifier le type de connexion/d'authentification, allez dans Microsoft SQL Management Studio et connectez-vous au serveur SQL, faites un clic droit sur le serveur SQL et sélectionnez Propriétés. Sélectionnez la page Sécurité et assurez-vous que le **Mode d'authentification SQL Server et Windows** est sélectionné si une authentification SQL est sélectionnée lors de l'installation de l'application Intel Unite® sur le serveur.



Si cette erreur continue de s'afficher, réinitialisez le mot de passe de **UniteServiceUser**. Utilisez Microsoft SQL Management Studio et connectez-vous au serveur SQL, accédez à **Sécurité** > **Connexions** et faites un clic droit sur **UniteServiceUser** pour ouvrir la fenêtre des **Propriétés de la connexion**. Saisissez un nouveau mot de passe et cliquez sur **OK** pour enregistrer les modifications.



12.4.2 Aucun serveur répertorié. Tentative de recherche dans l'enregistrement de service DNS : _uniteservice._tcp

Solution de contournement/Solution :

Cela peut se produire lorsque le concentrateur ne parvient pas à trouver l'enregistrement DNS. Aux fins de débogage, ouvrez la fenêtre de ligne de commande et exécutez la commande nslookup. Assurez-vous que le concentrateur peut faire un test de ping du serveur sur lequel le service DNS s'exécute et qu'un enregistrement de service DNS a été créé pour la solution Intel Unite®. L'enregistrement de service doit comporter les valeurs suivantes : **Service** : _uniteservice, **Protocole** : _tcp, **Numéro de port** : 443 et **Hôte offrant ce service :** FQDN du serveur d'entreprise.

12.4.3 Impossible d'établir une relation fiable pour le canal sécurisé SSL/TLS avec l'autorité uniteserverfqdn

La dernière version de la solution Intel Unite® accepte uniquement les certificats SHA-2 ou supérieurs. Contactez votre service informatique afin de vous assurer que le certificat du serveur Web émis est un certificat SHA-2 et que le cursus de certification est valide.
Pour un environnement de test, obtenez le certificat SHA-2 ou désactivez le chiffrement dans votre environnement.

- Pour utiliser Intel Unite® sans chiffrement, sautez les étapes suivantes qui fournissent des renseignements sur les liaisons de sites au port sécurisé 443, et installez SQL Server de Microsoft, puis préparez l'enregistrement de service DNS. Vous devez également vous assurer que le service se trouve sur le port 80 lorsqu'un enregistrement de service DNS est créé.
- Une autre façon d'ignorer la vérification du certificat est d'ajouter le registre du compte de la machine du concentrateur et du client.
  HKEY_LOCAL_MACHINE\software\Intel\Unite\AllowInsecureCertificates (DWORD) [1 si la vérification de l'algorithme du certificat doit être ignorée, 0 dans le cas contraire. (si la valeur est 0, le certificat d'entreprise devra obligatoirement utiliser un certificat SHA-2.)]

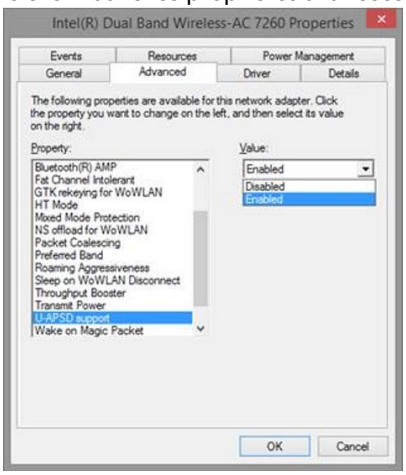
12.5 L'application client bloque au lancement/à la connexion

Exécutez l'application client avec un commutateur de débogage et enregistrez les données dans un journal. (Exécutez Intel Unite.exe /debug >logfile.txt)
Si le journal affiche le message « EXCEPTION: - Key not valid for use in specified state. » (EXCEPTION : -Clé non valide pour une utilisation dans l'état spécifié), fermez l'application et supprimez le fichier C:\Users\eaviles\AppData\Roaming\Microsoft\Crypto\RSA\[sid]\d046df.

12.6 Zone d'avertissement : l'utilisateur peut constater des délais de connexion plus longs que d'habitude ou des écrans de mise jour périodiques lents.

Cause initiale :

Il s'agit d'un bogue qui concerne certains points d'accès sans fil lorsque la fonction d'économie d'énergie automatique non planifiée est activée. Consultez la page http://www.intel.fr/content/www/fr/fr/support/network-and-i-o/wireless-networking/000005615.html.
Solution de contournement : ce problème peut être résolu en mettant à jour le microprogramme du point d'accès sans fil. Dans la plupart des entreprises, il n'est pas facile de la faire. En dernier recours, vous pouvez désactiver cette option sur le client dans les propriétés avancées du pilote sans fil.



12.7 Zone d'avertissement : lenteur du serveur PIN

Solution de contournement/Solution : le serveur d'entreprise gère l'attribution des codes PIN et cherche les codes PIN permettant de se connecter aux salles. Pour des raisons de sécurité, la fréquence à laquelle un utilisateur peut demander des codes PIN et interroger les codes PIN de la base de données est limitée à l'aide d'un algorithme exponentiel de désactivation. Le mécanisme de désactivation surveille les tentatives en fonction de l'adresse IP de l'utilisateur et du nombre de tentatives.

Les serveurs de production peuvent utiliser des équilibreurs de charge pour aider à gérer la charge et maintenir la redondance de l'environnement. L'équilibreur de charge redirige le trafic vers les serveurs Web approprié. Il peut alors sembler que le serveur Web reçoit des demandes de la même adresse IP, ce qui déclenche les algorithmes de désactivation.

La base de données contient une procédure stockée (*spGetPinBackoffTime*) qui renvoie le retard calculé en secondes au serveur Web. Cette fonctionnalité peut être désactivée, la procédure stockée revient donc toujours à 0. Cela désactive alors l'algorithme de désactivation de sécurité.

12.8 Dépannage du client Mac

Lancez l'application Intel Unite® (/Applications/Utilitaires) depuis le terminal pour voir les messages de débogage.
/pathToUnite/Intel\ Unite.app/Contents/MacOS/Intel\ Unite
Cette application démarre alors et les informations de débogage s'affichent sur le terminal.

12.8.1 Erreur de connexion du serveur d'entreprise -1003 : impossible de trouver un serveur avec le nom d'hôte spécifié.

Solution de contournement/Solution : assurez-vous que le domaine de recherche DNS est défini correctement.
Si un utilisateur définit un serveur DNS, mais n'indique pas de domaine de recherche, lorsque le Mac tente d'effectuer une découverte automatique, il n'y a aucun suffixe de domaine DNS parmi lesquels faire une recherche. Si aucun domaine de recherche DNS n'est défini, l'application Intel Unite® ne peut pas en ajouter pour la découverte automatique ou en tant qu'entrée statique *uniteservice*. À moins que la découverte automatique ne fonctionne avec *_uniteservice._tcp*, le client ne pourra pas trouver le serveur d'entreprise. La solution la plus simple consiste à ajouter un domaine de recherche DNS (qui devrait correspondre à l'enregistrement de service DNS), mais il est également possible de définir le serveur d'entreprise dans les paramètres *plist*.
Utilisez la commande de terminal suivante :
defaults write com.intel.Intel-Unite EnterpriseServer monServeur.monDomaine.monTLD

12.8.2 Erreur de connexion du serveur d'entreprise -1001 : la demande a expiré

Solution de contournement/Solution : cette erreur peut être due aux deux motifs suivants :

1. Un problème semble exister avec le service Web du serveur d'entreprise.
2. Le Mac fait face à des problèmes réseau au moment de se connecter au serveur.

La première étape pour résoudre le problème consiste à chercher le service Web dans le journal de débogage. Cherchez https://votreserveur/Unite/CCService.asmx.
Copiez et collez cette URL dans Safari et confirmez que le Mac peut accéder au service Web. Cela permet de vérifier s'il y a un problème de réseau lors de la connexion au serveur et si le service Web sur le serveur d'entreprise s'exécute bien.

12.8.3 Erreur de connexion au serveur d'entreprise -1200 : une erreur SSL s'est produite et une connexion sécurisée au serveur ne peut pas être établie.

Contactez votre service informatique pour obtenir les certificats SHA-2 requis par la solution Intel Unite®.

12.9 L'application Intel Unite® pour Mac OS est supprimée/désinstallée de l'appareil client et une version alternative ou plus récente de l'application Intel Unite® est installée. Toutefois, les anciennes propriétés d'installation sont conservées.

L'application Intel Unite® pour appareils clients Mac respecte les conventions générales OS X. Ainsi, les paramètres utilisateurs ne sont pas effacés lorsque l'application est supprimée.

Solution de contournement/Solution :

Désinstallez l'application Intel Unite® de l'appareil client. Il existe deux façons de supprimer ces paramètres et de revenir à un état propre.

1. À partir du terminal, (/Applications/Utilitaires), saisissez la commande suivante :

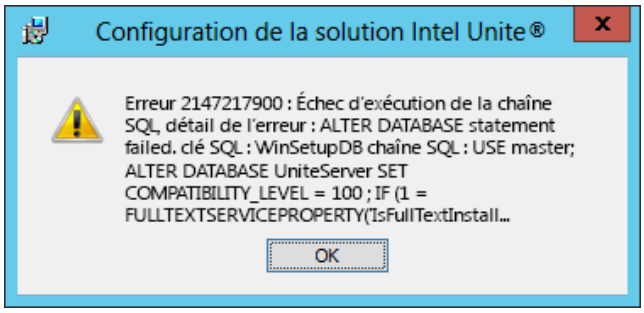
   defaults delete com.intel.Intel-Unite

2. À partir du Finder, supprimez le fichier ~/Library/Preferences/com.intel.Intel-Unite.plist.

   Redémarrez le système. Les fichiers Plist sont lourdement mis en cache par les systèmes d'exploitation récents. En règle générale, vous ne pouvez pas les supprimer et faire en sorte que le système d'exploitation détecte le changement.

12.10 Erreur 2147217900 : l'exécution de la chaîne SQL a échoué.

Cette erreur survient lorsque le programme d'installation du serveur Intel Unite® est exécuté et que la base de données Unite existe déjà, mais que le nom du serveur est vide.



Solution de contournement/Solution :
Le programme d'installation affiche une erreur si la base de données existe déjà dans le cluster. Pour résoudre cette erreur, supprimez la base de données, vérifiez que vous disposez de droits DBAdmin et lancez à nouveau le programme d'installation.

12.11 Message d'erreur : « Erreur de base de données »

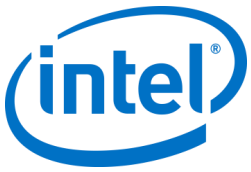
Si un administrateur informatique choisit l'option « Envoyer un jeton » sur la console d'administration, mais que le message d'erreur « Erreur de base de données » s'affiche, il est probable que les paramètres du serveur SMTP sont incorrects. Vérifiez les paramètres du serveur de messagerie SMTP.

12.12 Le portail Web d'administration ne s'affiche pas correctement (composants manquants)

Après la mise à niveau du logiciel Intel Unite®, le portail Web d'administration ne s'affiche pas dans son intégralité : des composants manquent, notamment des champs de texte, des options ou des icônes. Cela est dû au blocage des types MIME par l'option de filtrage des demandes d'IIS.

Solution de contournement/Solution :

1. Ouvrez le Gestionnaire IIS.
2. Affichez les propriétés du serveur IIS.
3. Cliquez sur **Types MIME**, puis ajoutez l'extension JSON :



- Extension de nom de fichier : .json
- Type MIME : application/json

4. Revenez aux propriétés du serveur IIS.
5. Cliquez sur **Mappages de gestionnaires**.
    - Ajoutez un mappage de scripts.
    - Chemin d'accès à la demande : *.json
    - Exécutable : C:\WINDOWS\system32\inetsrv\asp.dll
    - Nom : JSON
6. Dans le volet **Connexions**, accédez à la connexion, au site, à l'application ou au répertoire dont vous souhaitez modifier les paramètres de filtrage des demandes.
7. Dans le volet **Accueil**, double cliquez sur **Filtrage des demandes**.
8. Repérez Autoriser une extension de nom de fichier.
9. Ajoutez les quatre extensions suivantes :
    - .json
    - .less
    - .woff
    - .woff2

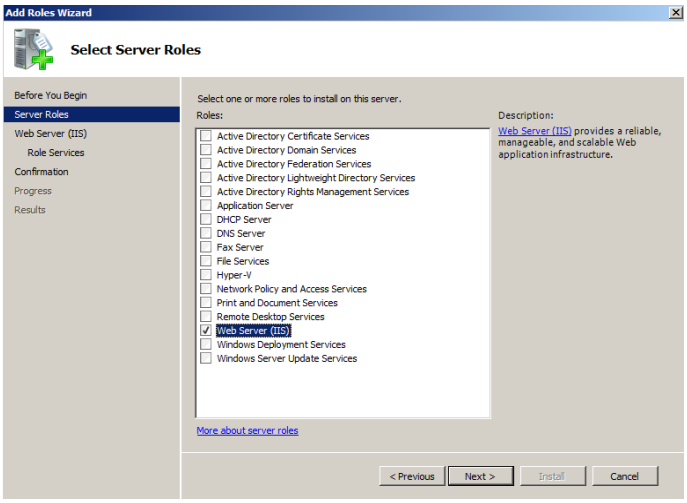
Annexe A. Préparation du serveur d'entreprise

Activation de IIS

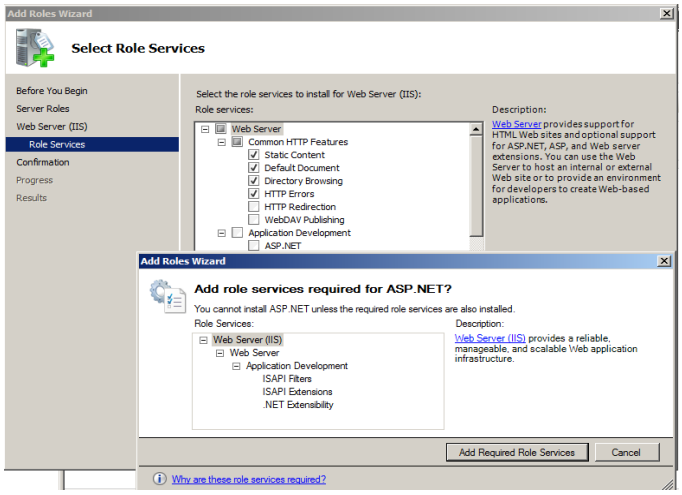
Pour Windows 2008 :

Sous Windows Server 2008, vous devez télécharger la mise à jour de .NET Framework 4.5 (https://www.microsoft.com/fr-fr/download/details.aspx?id=40779)

- Cliquez sur **Démarrer**, pointez sur **Outils d'administration**, puis cliquez sur **Gestionnaire de serveur**.
- Sous **Résumé des rôles**, cliquez sur **Ajouter des rôles**.
- Utilisez l'**Assistant Ajout de rôles** pour ajouter le rôle **Serveur Web (IIS)** (cochez cette case).



- Cliquez sur **Suivant** jusqu'à ce que la fenêtre **Sélectionner les services de rôle** s'affiche.
- Dans la section **Développement d'application**, vérifiez que ASP.NET est sélectionné. Sinon, sélectionnez-le. Veuillez noter que ASP.NET n'est pas sélectionné par défaut. **Ajoutez les services de rôle requis** pour ASP.NET. Vous aurez également besoin de ASP.NET 4.5.



- Une fois le rôle créé, dans le menu **Rôles**, accédez à **Serveur Web (IIS)**. À droite du volet, accédez au **Gestionnaire des services Internet (IIS)** et sélectionnez votre serveur dans le volet de gauche **Connexions**.

  Référence : Lien vers la bibliothèque Windows Server Installation d'IIS sur Windows Server 2008

  Remarque : la dernière version de la solution Intel® Unite™ accepte uniquement les certificats SHA-2 ou supérieurs. Contactez votre service informatique afin de vous assurer que le certificat du serveur Web émis est un certificat SHA-2 et que le cursus de certification est valide.

  Pour un environnement de test, contactez l'équipe responsable des certificats pour obtenir un certificat SHA-2 ou désactiver le chiffrement.
  - Pour utiliser Intel® Unite™ sans chiffrement, sautez les étapes suivantes qui fournissent des renseignements sur les liaisons de sites au port sécurisé 443, et installez SQL Server de Microsoft, puis préparez l'enregistrement de service DNS. Vous devez également vous assurer que le service se trouve sur le port 80 lorsqu'un enregistrement de service DNS est créé.
  - Vous pouvez également ignorer la vérification du certificat en ajoutant la clé de registre du compte de la machine du concentrateur et du client. HKEY_LOCAL_MACHINE\software\Intel\Unite\AllowInsecureCertificates (DWORD) [1 si la vérification de l'algorithme du certificat doit être ignorée, 0 dans le cas contraire. (si la valeur est 0, le certificat d'entreprise devra obligatoirement utiliser un certificat SHA-2.)]

- Pour assigner le certificat, dans le volet de gauche **Connexions**, développez Sites et cliquez sur **Site Web par défaut**.
- Dans le volet de droite **Actions**, sélectionnez **Liaisons** (sous Modifier le site).
- Dans la fenêtre **Liaisons de sites**, cliquez sur **Ajouter**.
- Utiliser les informations suivantes :
  - Type : https (remarque : pas http)
  - Adresse IP : Toutes non attribuées
  - Port : 443
  - Nom d'hôte : (laisser vierge)
  - Certificat SSL : utilisez le certificat SSL qui a été installé aux étapes suivantes.

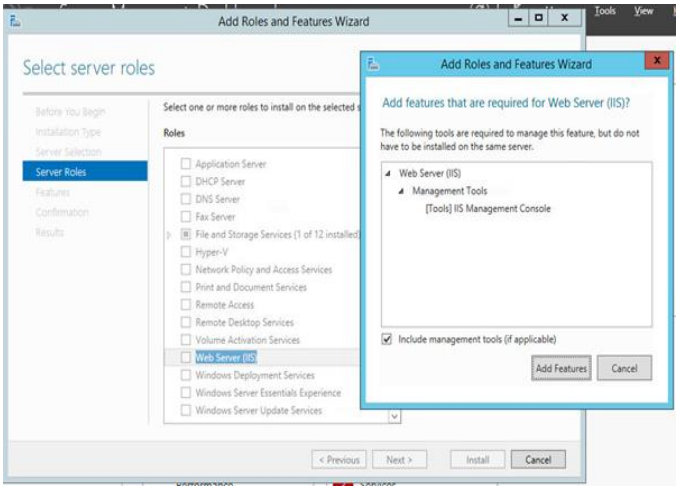
Cliquez sur **OK**.

Windows 2012 :

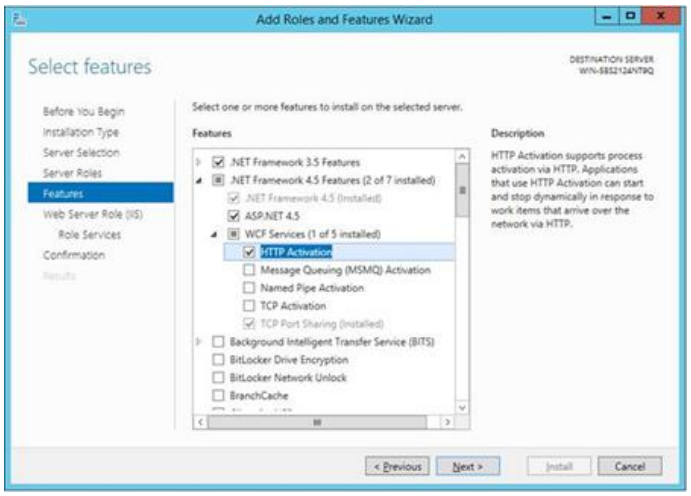
- Ouvrez le **Gestionnaire de serveur**.

- Dans le menu **Gérer**, sélectionnez **Ajouter des rôles et fonctionnalités**.
- Sélectionnez **Installation basée sur un rôle ou une fonctionnalité.**
- Sélectionnez le serveur approprié (local est sélectionné par défaut).
- Sélectionnez **Serveur Web (IIS)** et **Ajouter des fonctionnalités** (nécessaire pour le serveur Web [IIS], puis cliquez sur **Suivant**.

REMARQUE : si vous avez besoin de plus de renseignements sur la façon de demander un certificat de serveur Internet pour le serveur Unite, consultez la page Microsoft https://technet.microsoft.com/en-us/library/cc732906.aspx et suivez les étapes concernant l'obtention d'un certificat SSL signé.



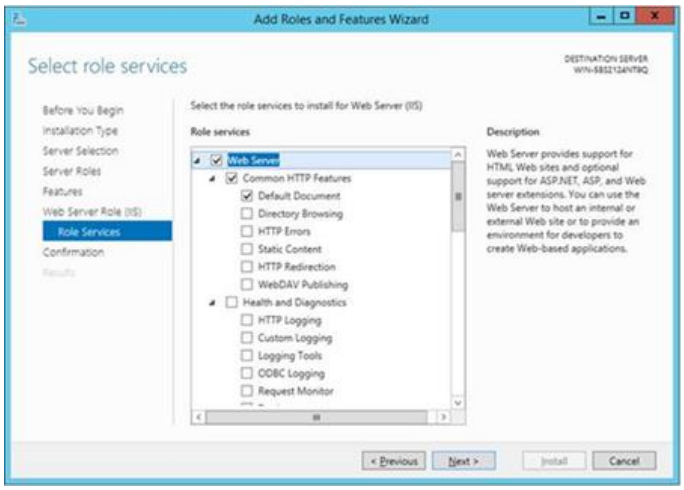
- Sous Fonctionnalités, ajoutez les fonctionnalités suivantes pour IIS (car elles ne sont pas activées par défaut) :
  - Fonctionnalités de .NET Framework 3.5
  - ASP.NET 4.5
  - Services WCF
  - Activation HTTP (ajoutez les fonctionnalités requises pour l'activation HTTP lorsque vous y êtes invité et cliquez sur **Suivant**).



Remarque : .NET 3.5 peut générer une erreur lors de l'installation. Indiquez un autre chemin source si l'ordinateur cible n'a pas accès à Windows Update. Cliquez sur le lien **Spécifier un autre**

chemin d'accès source pour indiquer l'emplacement du dossier **\sources\sxs** sur le support d'installation.
Référence : https://technet.microsoft.com/fr-fr/library/dn482071.aspx

- Sur la page Services de rôle, ajoutez **Serveur Web (IIS)** en tant que rôle à votre serveur ou acceptez la valeur par défaut.
- Sélectionnez les services de rôle suivants pour installer le serveur Web :
    - Fonctionnalités HTTP communes
    - Document par défaut



- Cliquez sur **Suivant** pour continuer et cliquez sur **Installer** dans la fenêtre suivante pour installer les rôles et les fonctionnalités sélectionnés.
- Une fois le rôle créé, dans le menu **Rôles**, accédez à **Serveur Web (IIS)**. À droite du volet, accédez au **Gestionnaire des services Internet (IIS)** et sélectionnez votre serveur dans le volet de gauche, **Connexions**.

  Remarque : la dernière version de la solution Intel Unite® accepte uniquement les certificats SHA-2 ou supérieurs. Contactez votre service informatique afin de vous assurer que le certificat du serveur Web émis est un certificat SHA-2 et que le cursus de certification est valide.

  Pour un environnement de test, désactivez le chiffrement ou créez un certificat SHA 2 auto-signé.
    - Pour utiliser Intel Unite® sans chiffrement, sautez les étapes suivantes qui fournissent des renseignements sur les liaisons de sites au port sécurisé 443, et installez SQL Server de Microsoft, puis préparez l'enregistrement de service DNS. Vous devez également vous assurer que le service se trouve sur le port 80 lorsqu'un enregistrement de service DNS est créé.
    - Exécutez la commande PowerShell suivante en tant qu'administrateur.
        - New-SelfSignedCertificate –dnsname “nomdevotreserveur” –CertStoreLocation cert:\LocalMachine\My ; « nomdevotreserveur » est le FQDN du serveur d'entreprise.
    - Vous pouvez également ignorer la vérification du certificat en ajoutant la clé de registre du compte de la machine du concentrateur et du client. HKEY_LOCAL_MACHINE\software\Intel\Unite\AllowInsecureCertificates (DWORD) [1 si la vérification de l'algorithme du certificat doit être ignorée, 0 dans le cas contraire. (si la valeur est 0, le certificat d'entreprise devra obligatoirement utiliser un certificat SHA-2.)]

- Pour assigner le certificat, dans le volet de gauche **Connexions**, développez Sites et cliquez sur **Site Web par défaut**.

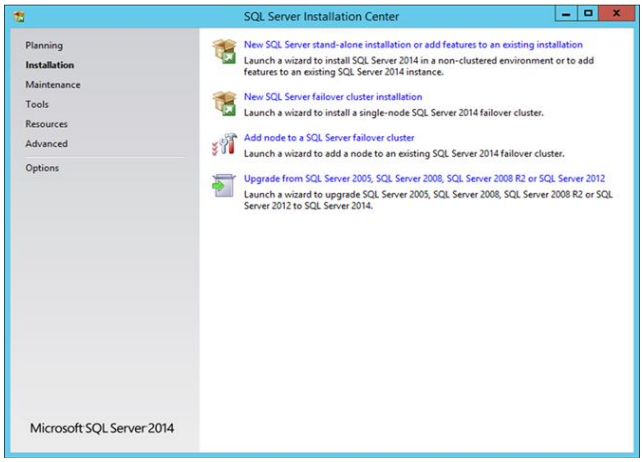
- Dans le volet de droite **Actions**, sélectionnez **Liaisons** (sous Modifier le site).
- Dans la fenêtre **Liaisons de sites**, cliquez sur **Ajouter**.
- Utiliser les informations suivantes :
    - Type : https (remarque : pas http)
    - Adresse IP : Toutes non attribuées
    - Port : 443
    - Nom d'hôte : (laisser vierge)
    - Certificat SSL : (sélectionnez le certificat que vous avez installé aux étapes précédentes.)
    - Cliquez sur **OK**.
- Cliquez sur **Fermer**.

Référence : Lien vers la bibliothèque Windows Server Installation d'IIS sur Windows Server 2012
Remarque concernant le port 443 : le service Web de l'application Intel Unite® communique avec les clients et les concentrateurs à l'aide du port 443. Veillez donc à ce que ce port soit activé comme indiqué ci-dessus.

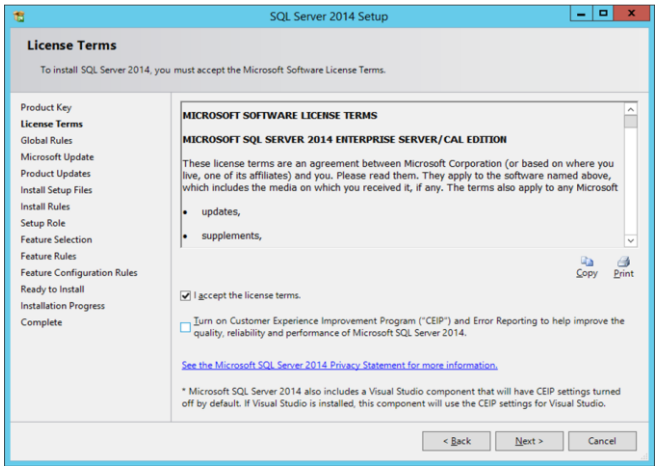
Installation de Microsoft SQL Server

Le serveur d'entreprise nécessite MS SQL version 2008 R2 ou supérieure pour s'exécuter. Vous pouvez installer un nouveau serveur SQL dédié si vous souhaitez exécuter un « environnement d'essai » pour vous familiariser avec l'application ; cependant, cela n'est pas obligatoire. L'application Intel Unite® crée sa propre base de données, ses tables de données et ses index dans votre base de données existante, sans perturber les autres tables ou données existantes.
Consultez les instructions ci-dessous pour installer MS SQL 2014.

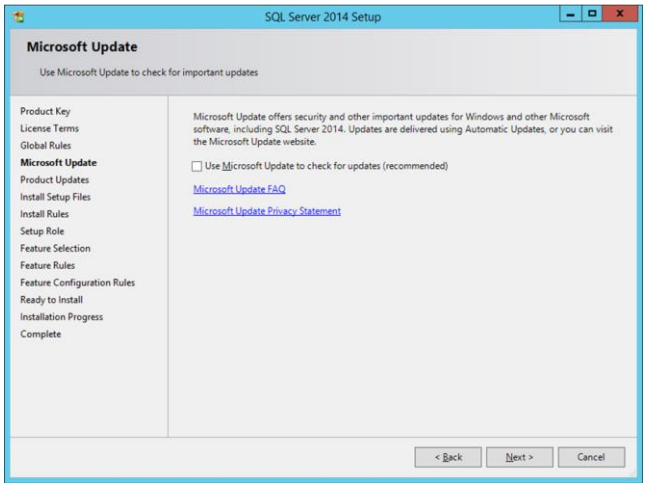
- Exécutez la configuration du serveur SQL et ouvrez le centre d'installation du serveur SQL. Cliquez sur **Installation** dans le volet de gauche et sélectionnez **Nouvelle installation autonome SQL Server ou ajout de fonctionnalités à une installation existante**.



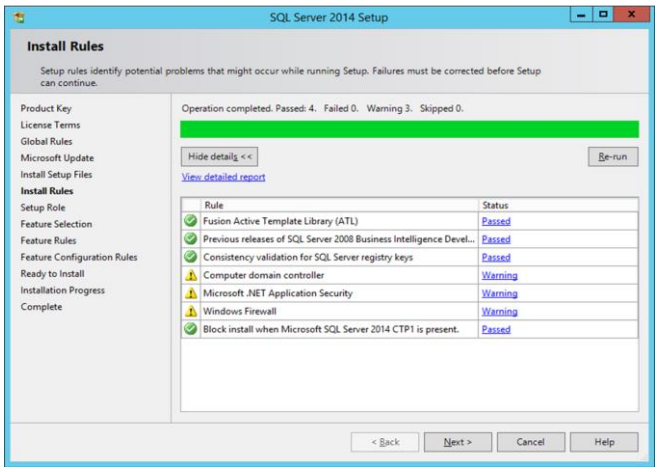
- Saisissez la clé du produit, acceptez les conditions de licence et cliquez sur **Suivant**.



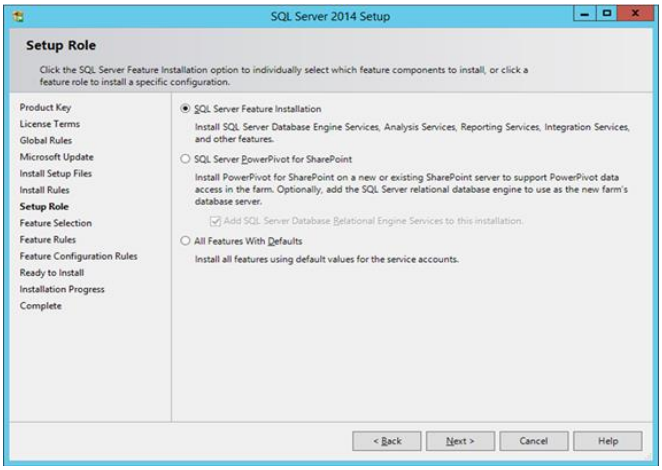
- Sélectionnez **Utiliser Microsoft Update pour rechercher les mises à jour (recommandé)** pour chercher les mises à jour disponibles, puis cliquez sur **Suivant**. Dans la fenêtre suivante, l'écran de configuration recherchera les mises à jour de produit et installera les mises à jour nécessaires. Pour continuer, cliquez sur **Suivant**.



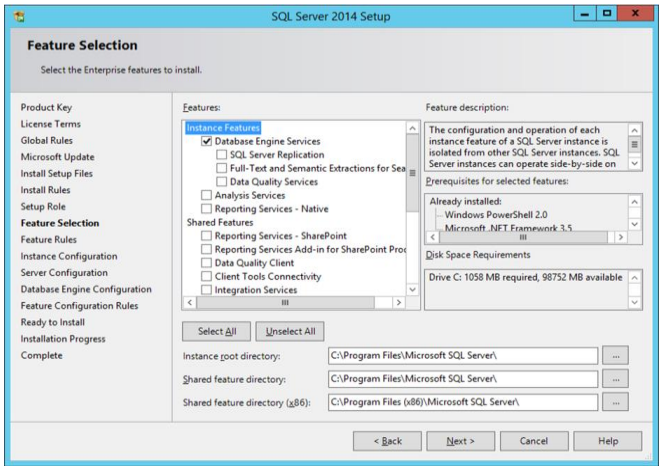
- Le paramétrage SQL cherche les défauts et les exigences éventuelles à respecter avant l'installation. Cliquez sur **Suivant** pour continuer.



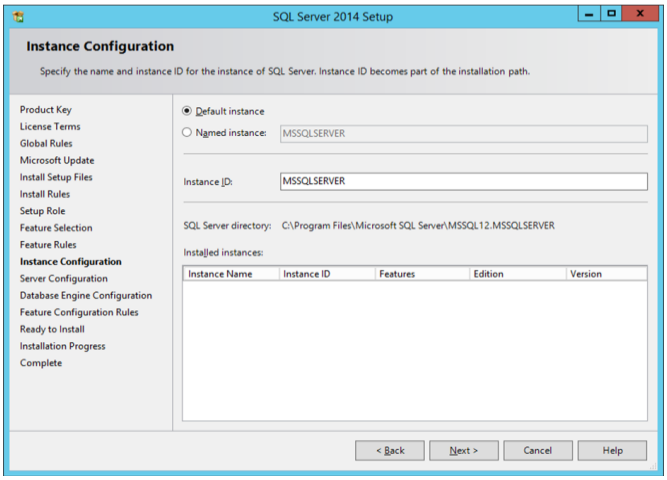
- Sélectionnez **Installation de fonctionnalités SQL Server** et cliquez sur **Suivant**.



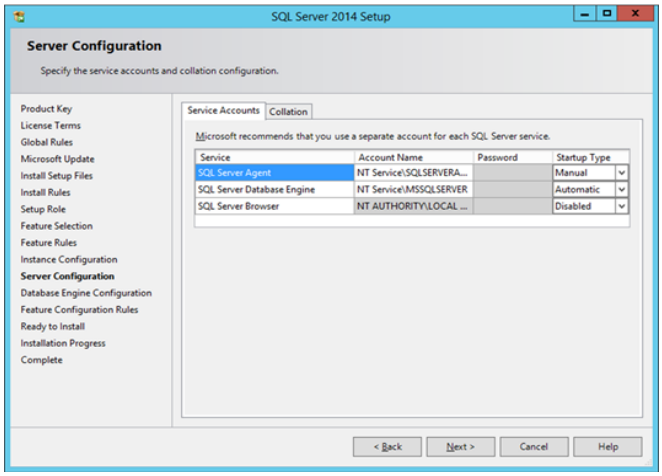
- Dans la fenêtre de **sélection des fonctionnalités**, sélectionnez **Services Moteur de base de données**, **Outils de gestion - Complet**, puis cliquez sur **Suivant**.



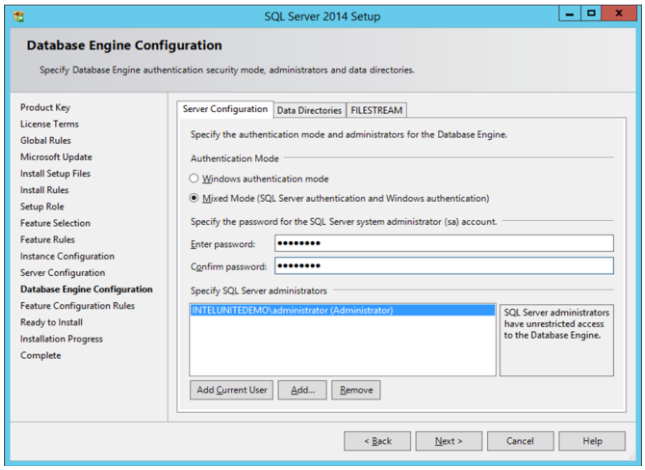
- Indiquez le nom et l'ID d'instance du serveur SQL, puis cliquez sur **Suivant**.



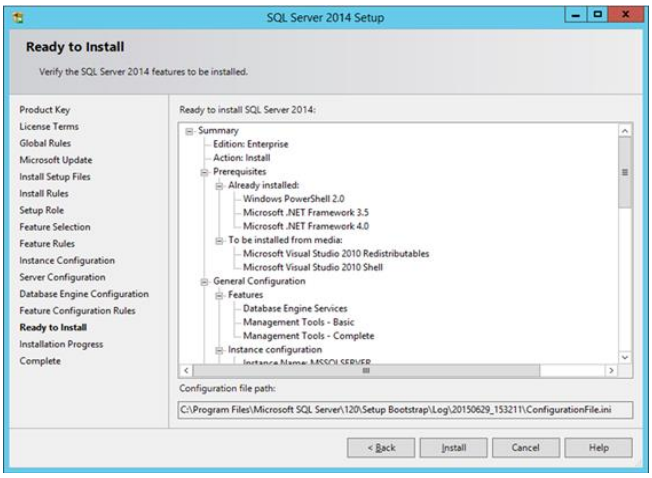
- Indiquez les comptes de service de chaque service, puis cliquez sur **Suivant** pour continuer.



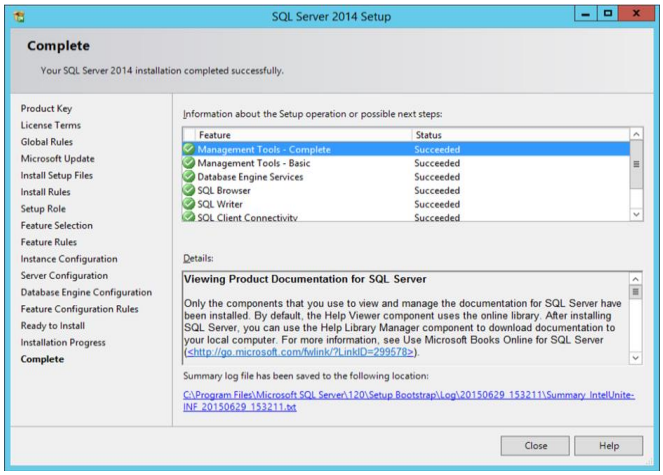
- Sélectionnez le mode mixte d'authentification (qui inclut l'authentification SQL et Windows), indiquez les administrateurs du serveur SQL, puis cliquez sur **Suivant**.



- Vérifiez les fonctionnalités à installer, puis cliquez sur **Installer**.



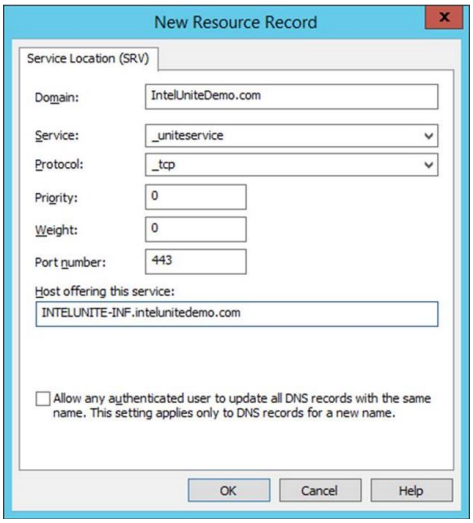
- Une fois l'installation terminée, **fermez** la boîte de dialogue.



Création d'un enregistrement de service DNS

Le concentrateur ou les clients localiseront le serveur d'entreprise à l'aide du service DNS au cours d'une recherche automatique du serveur d'entreprise. Vous pouvez également effectuer une recherche manuelle, mais il est vivement conseillé d'utiliser un DNS. Si vous envisagez d'indiquer le nom d'hôte du serveur d'entreprise manuellement pendant l'installation du concentrateur et du client, vous pouvez ignorer cette rubrique.
Lors de l'utilisation d'un enregistrement de service DNS, le concentrateur ou le client cherchera le service intitulé _uniteservice._tcp parmi les enregistrements de service DNS _uniteservice._tcp.exemple.com 86400 IN 0 5 443 uniteserver.exemple.com.
Pour ajouter un enregistrement de service DNS dans Microsoft Windows :

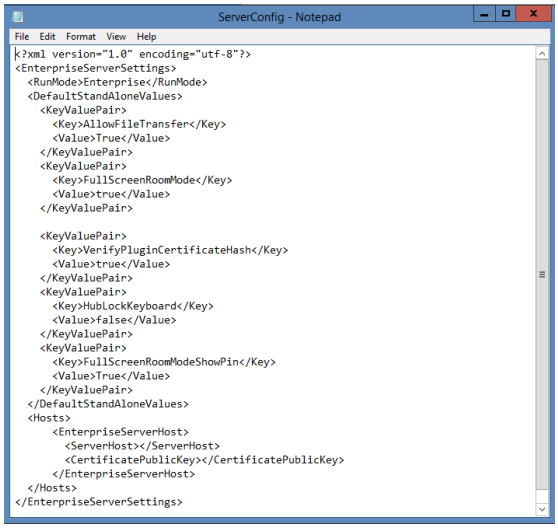
- Sur votre serveur DNS, ouvrez le Gestionnaire DNS.
- Développez les zones de recherche directe (volet de gauche).
- Effectuez un clic droit sur la zone et sélectionnez « Autres nouveaux enregistrements... »
    - Dans **Choisir un type d'enregistrement de ressource**, sélectionnez **Emplacement du service (SRV)**, puis sélectionnez **Créer un enregistrement**.
    - Pour **Service**, saisissez : _uniteservice
    - Pour **Protocole**, saisissez : _tcp
    - Pour **Port**, saisissez : 443
    - Pour Hôte offrant ce service, saisissez le nom d'hôte ou l'adresse IP du ou des serveurs d'entreprise.



REMARQUE : consultez la page Microsoft suivante pour en savoir plus sur la façon de configurer un serveur DNS pour utiliser des redirecteurs : https://technet.microsoft.com/en-us/library/cc754941.aspx

Annexe B. Exemple de ServerConfig.xml

Le fichier ServerConfig.xml est créé pendant l'installation des composants du concentrateur et du client sur le logiciel Intel Unite®. L'emplacement par défaut du fichier xml est C:\Program Files (x86)\Intel\Intel Unite\Hub ou C:\Program Files (x86)\Intel\Intel Unite\Client pour le concentrateur et le client, respectivement.
Le fichier est modifié lorsque vous **spécifiez le serveur** et que vous saisissez le nom d'hôte du serveur ou quand vous saisissez la **Clé publique** manuellement lors de l'installation du logiciel Intel Unite® sur le concentrateur ou le client.
Si vous souhaitez modifier le fichier serverconfig.xml après l'installation, accédez au dossier où le fichier se trouve et apportez les modifications nécessaires.



Si un serveur est défini dans le fichier ServerConfig.xml, il aura priorité sur l'enregistrement de service DNS.

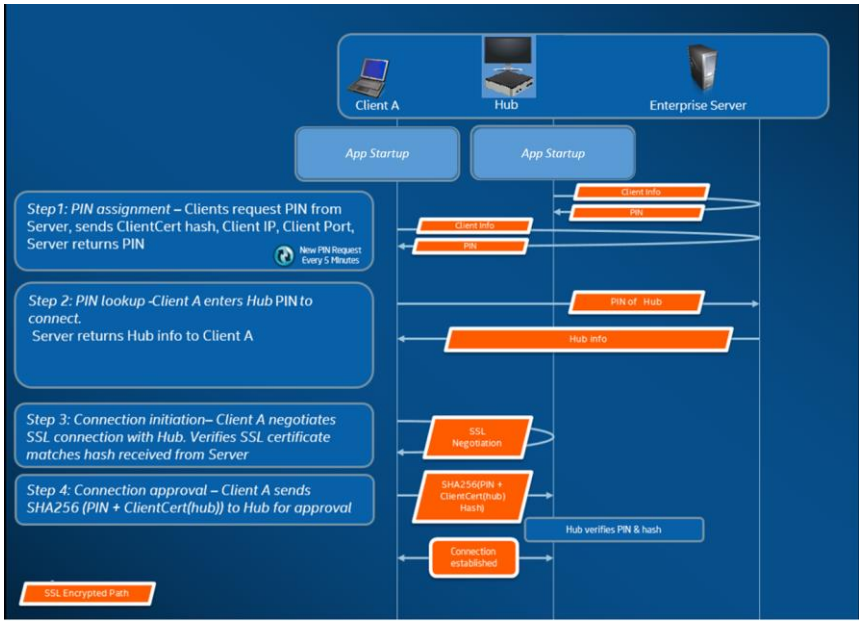
Annexe C. Solution Intel Unite® – Présentation du processus de sécurité

Logiciel Intel Unite® - Flux de sécurité

Cette rubrique décrit brièvement les éléments de sécurité de l'application Intel Unite®. La sécurité de la connexion est abordée pour les quatre étapes suivantes :

1. Attribution de codes PIN
2. Recherche de codes PIN
3. Démarrage de la connexion
4. Approbation de la connexion

L'image suivante est un aperçu général de la façon dont les applications du client (doté de la technologie Intel® vPro™) et du concentrateur reçoivent de manière sécurisée les codes PIN du serveur d'entreprise, saisissent les codes PIN et établissent une connexion.



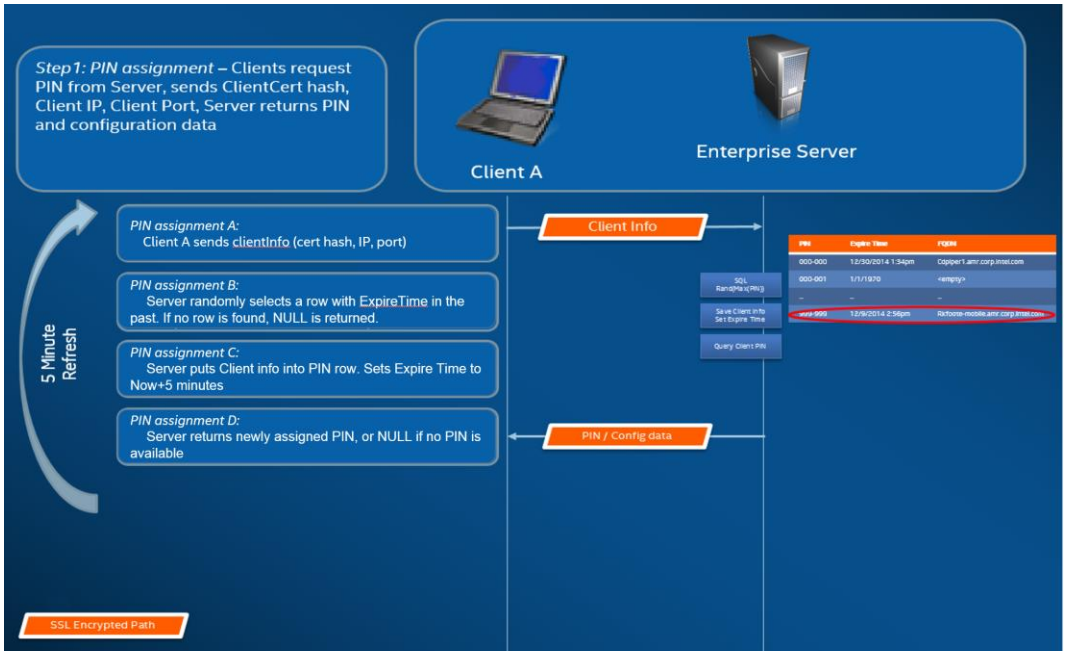
Étape 1 : Attribution de codes PIN

L'image ci-dessous illustre le processus d'attribution des codes PIN. Pendant le processus, toutes les communications réseau sont cryptées en SSL sur un service Web (TCP 443).
En plus de recevoir des codes PIN, le concentrateur et le client enregistrent leurs informations de connexion et une clé publique sur le serveur. La clé publique est utilisée à la connexion pour vérifier que chaque composant communique bien avec la cible correspondante.

Remarque : l'attribution de codes PIN pour le client (doté de la technologie Intel® vPro™) et le concentrateur suit le même flux.

Veuillez également noter ce qui suit :

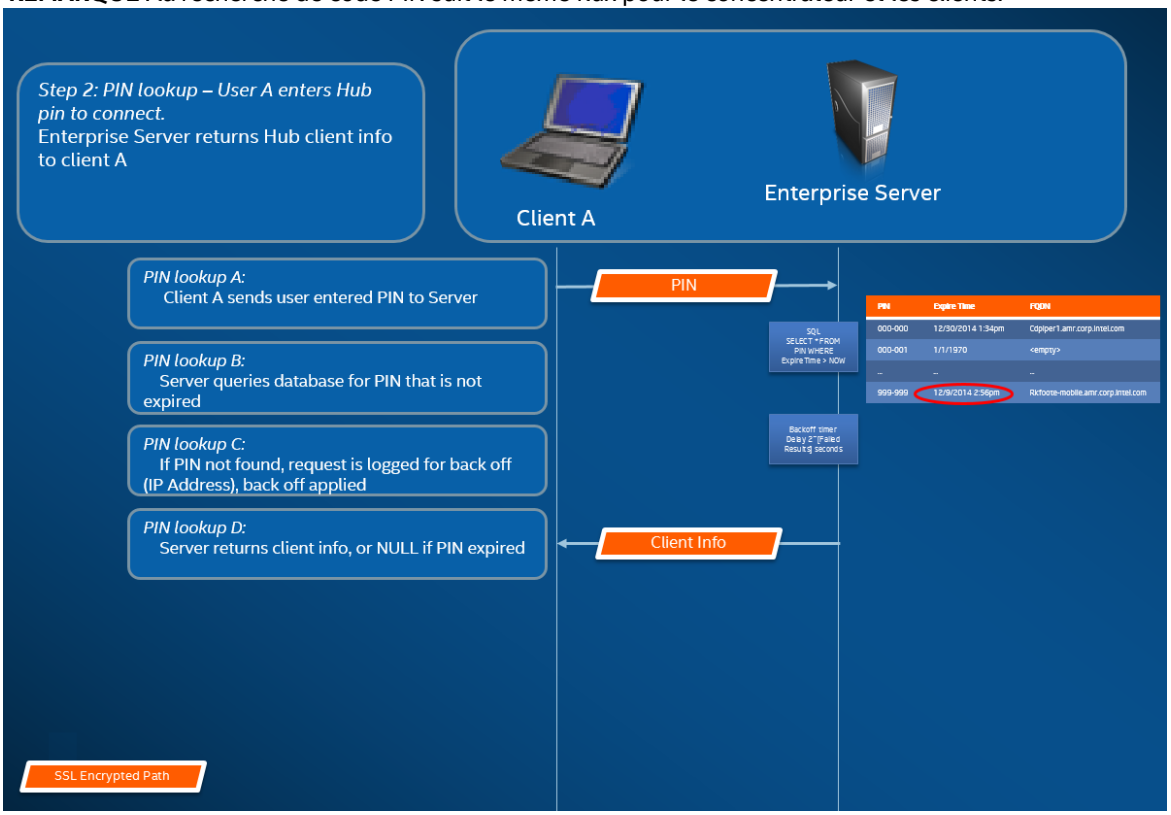
- L'intervalle d'actualisation du code PIN peut être configuré.
- Lorsque le concentrateur ou le client envoie des informations de connexion, les plages d'adresses IP dans l'hôte local (127.0.0.0/8 et 169.254.0.0/16) sont ignorées.
- Le port TCP peut être configuré selon le client ou le concentrateur, ou activé via un profil du portail Administrateur. Le comportement par défaut est de laisser le système d'exploitation attribuer un port.
- Les codes PIN expirés sont encore accessibles pendant 15 secondes.
- Les codes PIN expirés ne sont pas réattribués pendant 5 minutes après leur expiration. Cela permet d'éviter que les utilisateurs se connectent malencontreusement au mauvais affichage.



Étape 2 : Recherche de codes PIN

L'image ci-dessous décrit la manière dont les codes PIN sont intégrés au serveur d'entreprise. Lors de la recherche de code PIN, toutes les communications réseau sont cryptées en SSL sur un service Web (TCP 443).
Lorsqu'un utilisateur saisit le code PIN d'une cible dans le client, le client envoie le code PIN au serveur d'entreprise pour obtenir les informations de connexion. Lorsque la recherche réussit, le serveur d'entreprise renvoie les informations de connexion valides de la cible. La cible peut être un concentrateur ou un client (doté de la technologie Intel® vPro™) exécutant le logiciel Intel Unite®.
Outre les informations de connexion, la clé publique de la cible est aussi fournie, de sorte que l'application client puisse vérifier qu'elle communique avec la bonne cible.

REMARQUE : la recherche de code PIN suit le même flux pour le concentrateur et les clients.

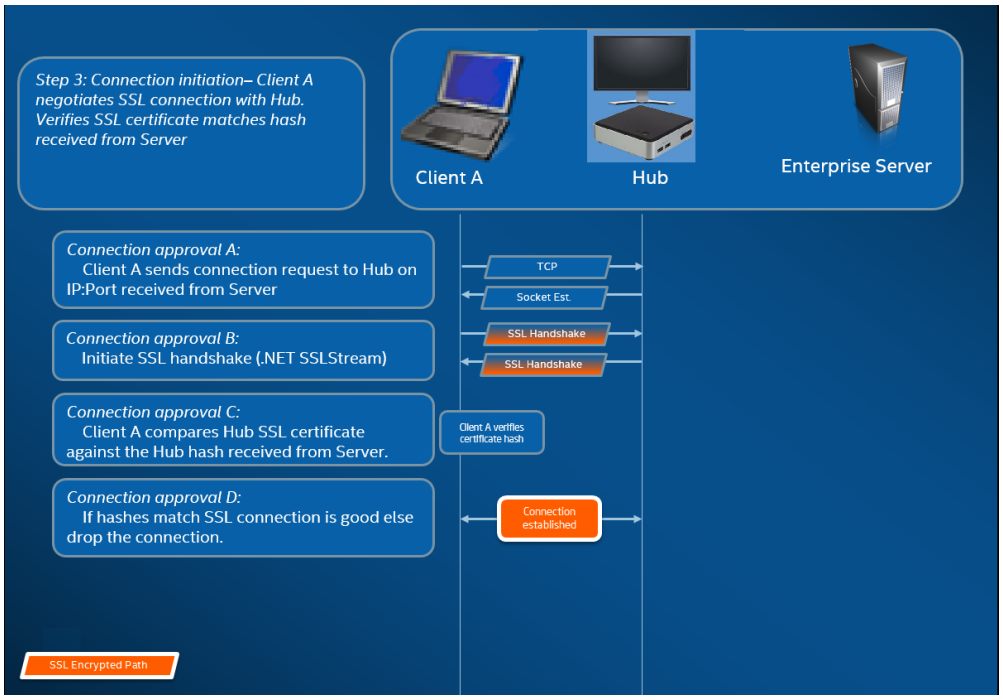


Désactivation de la recherche de code PIN

Pour éviter les tentatives de collecte de codes PIN depuis le serveur d'entreprise, les tentatives échouées sont enregistrées. Un utilisateur a droit à 3 tentatives échouées sur une période de 10 secondes avant que le processus de désactivation n'impose un délai de réponse (2^x secondes, où x est le nombre de tentatives échouées sur une période de 5 minutes).

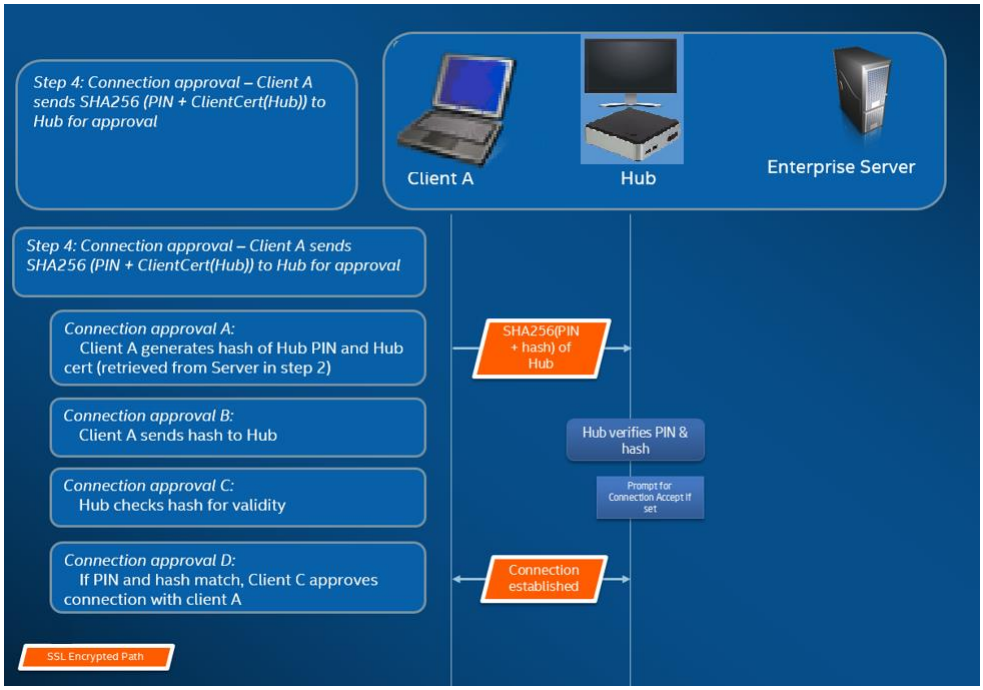
Étape 3 : Lancement de la connexion

L'image ci-dessous illustre le lancement d'une connexion. Le client lance une connexion TCP poste à poste avec la cible (un concentrateur ou un client avec la technologie Intel® vPro™ exécutant le logiciel Intel Unite®), puis démarre une négociation SSL. Le certificat fourni par la cible est haché et comparé au hachage reçu par le client à l'étape 2. Ce type de validation empêche les attaques et évite également les situations où les adresses IP des clients DHCP changent.



Étape 4 : Autorisation de connexion

L'image ci-dessous montre comment la connexion est établie entre le client et la cible, qui peut être un concentrateur ou un client (avec la technologie Intel® vPro) exécutant le logiciel Intel Unite®. Une fois que la cible a vérifié le code PIN et le certificat du client, elle accepte la connexion et une connexion est établie entre le client et la cible.



Annexe D. Solution Intel Unite® – Équilibreur de charge

Cette section décrit brièvement comment contourner la désactivation du PIN derrière l'équilibreur de charge/le proxy.
Si vous êtes derrière un équilibreur de charge, assurez-vous que la procédure stockée dans SQL dbo.spGetPinBackoffTime **revient toujours à 0.**
Étapes :

- Modifiez la procédure stockée dbo.spGetPinBackoffTime. Vous pouvez ajouter des commentaires partout et utiliser « sélectionner 0 » à la fin.
- Exécutez le script.

Si vous n'êtes pas derrière un équilibreur de charge, assurez-vous que la procédure stockée est définie sur la valeur par défaut.