



**GROUPEMENT
HOSPITALIER
DE TERRITOIRE**
LOIRE ATLANTIQUE

Gestion des Postes Clients et Equipements numériques

Les informations présentées sont destinées à décrire les principes de gestion du poste de travail standardisé au CHU de Nantes (CHUN).

Ce support rassemble les différentes informations techniques et organisationnelles destinées à la définition, au maintien, à la mise à jour et à la modification du standard, basé sur un socle normalisé.

Il présente :

- **Le principe de catégorisation**
 - Les postes sont regroupés selon leur similitude d'usage
- **Les contraintes concernant l'authentification de l'utilisateur pour accéder au poste client**
 - L'ouverture d'une session Windows "standard" après insertion carte (le poste personnel) ou le déverrouillage d'une session Windows générique après insertion carte (le poste partagé)
- **Les contraintes pour connecter un équipement au réseau CHU**
 - Installation d'un master Windows CHUN (suite acquisition marché publique ou fourniture par éditeur) pour un accès complet (domaine Microsoft CHUN, réseau de confiance "trusted") ou système géré par le fournisseur avec un accès réseau restreint (pas de jonction au domaine, pas d'outils CHUN, réseau "untrusted" avec accès basés sur matrice de flux réseau)
- **Le principe de qualification**
 - Tout matériel ou logiciel intégré au parc doit faire l'objet d'une qualification interne

Catégorisation des Equipements Numériques

Un environnement de travail standardisé CHU de Nantes est défini par la combinaison de cinq composants :

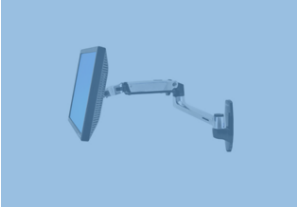


Support

Différents supports sont proposés\disponibles en fonction de l'usage et de la localisation du poste de informatique ;

La réponse aux besoins de mobilités des soignants et médecins (visite de patients, administration de médicaments, soins ...) est satisfait par la mise à disposition de postes informatiques sur chariots (chariot de visite, chariot médicament, chariot de soins ...), les postes localisés en salle de soins destinés à un usage d'affichage simple (peu ou pas d'interactions utilisateur) sont disposent généralement d'un support de type fixation murale etc...

Bras articulé



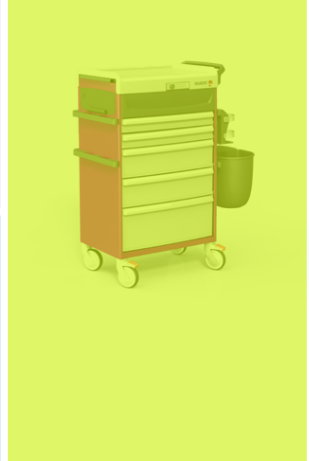
Chariot léger



Coque



Chariot Médicament



Fixation murale



Bureau



Mode d'authentification

Principe

Le CHU de Nantes fournit à chacun de ses agents une carte d'établissement (la "**carte gaia**") sur laquelle s'appuie la gestion des accès **logique** (poste de travail, applications ...) et **physique** (locaux, parking, restauration...).

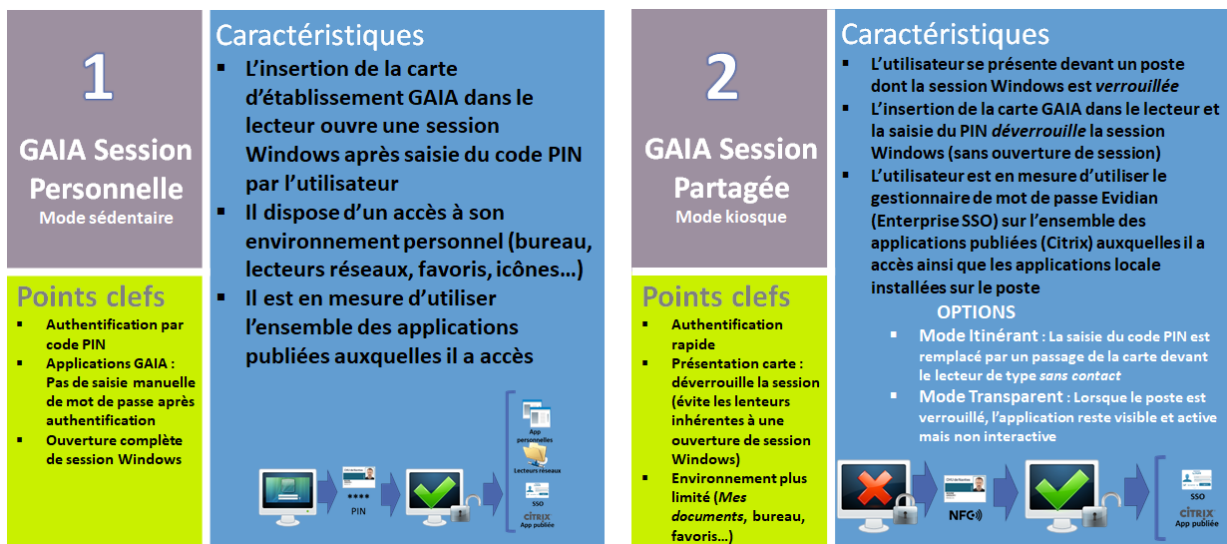
Pour accéder au poste et à son environnement système et applicatif, le CHU de Nantes utilise la solution Gaia (basée sur les produits Evidian Enterprise SSO et Authentication manager). Cette suite permet donc à l'utilisateur d'accéder à un environnement Windows et aux applications métier via l'utilisation d'une carte à puce propre au CHU de Nantes (carte d'établissement).

Après l'**authentification primaire** de l'utilisateur (code PIN), Entreprise SSO récupère dans le référentiel des données de SSO, les attributs de sécurité de l'utilisateur, tels que **les mots de passe** pour accéder à ses applications cibles. Ces attributs de sécurité sont **stockés de manière sécurisée** dans le référentiel des données de SSO puis rapatriés sur le poste de travail dans un cache de sécurité chiffré.

La solution de SSO va se substituer à l'utilisateur pour la saisie des credentials (identifiant et mot de passe) vers les applications référencées (grâce à un script d'identification des champs de saisie à configurer depuis les consoles Evidian).

La solution permet ainsi d'assurer la gestion des multiples mots de passe dès lors que l'utilisateur s'est authentifié au démarrage de sa session.

La solution Gaia installé sur un poste de travail peut être configuré en mode **Session personnelle (Sedentaire)** ou en mode **session partagée (kiosk)** :



En fonction du contexte d'utilisation de l'application (poste personnel ou partagé, application client lourd ou application publiée) l'authentification aux applications métiers est basée :

- Sur du SSO classique ActiveDirectory-Kerberos (Windows Integrated Authentication - WIA)
- Sur du SSO evidian (client SSO) : un agent (Evidian User Access), exécuté sur le poste de travail, capture les fenêtres d'authentification et saisie les champs identifiant/mot de passe en se basant sur les définitions techniques du script e-SSO contenu dans le container de l'utilisateur.

Détail de fonctionnement du mode Gaia Session Partagée

Par défaut, le principe du mode Session partagée (aka "kiosk") est le suivant:

1. Au démarrage initial du poste, le système Evidian assure une ouverture de session Windows automatique sans avoir à saisir le mot de passe (autologon avec un compte windows **générique**)
2. Avant l'apparition du bureau Windows, le système Evidian verrouille la session Windows, aucune action utilisateur n'est possible

Lorsqu'un utilisateur souhaite utiliser le poste:

1. Il insère sa carte d'établissement (carte "Gaia", à puce contact (historiquement IAS ECC, actuellement IDPrime) et sans contact RFID(MiFare classic)) dans le lecteur
2. il saisie son code PIN pour déverrouiller la **session Windows générique**
3. En arrière plan, l'agent Evidian se charge sous l'identité (login et mot de passe) du porteur de la carte
4. L'agent Evidian ferme toute les applications éventuellement ouverte par l'utilisateur précédent et réalise la connexion des lecteurs réseaux du porteur de la carte (fonction *FUSMap*)

Seul l'agent Evidian identifie le porteur de la carte, la session Windows est toujours celle du compte windows **générique**

L'agent Evidian connaît donc l'identité du porteur de la carte ; A partir de là, lorsqu'une fenêtre d'application connue par l'agent apparaît, celui-ci se substitue à l'utilisateur pour saisir son identifiant (login) et son mot de passe :

Exemple :

- Lorsque le client Citrix se lance, une fenêtre d'authentification apparaît, l'agent SSO capte cette fenêtre et rentre le login AD et le mot de passe de l'utilisateur à sa place ; Citrix est donc authentifié avec l'identité du porteur de la carte et lui affiche ses icônes de raccourcis d'applications sur le bureau
- Lorsque l'utilisateur lance une application installée sur le poste (client lourd) et que celle-ci est connue par le système Evidian, l'agent Evidian saisie à la place de l'utilisateur son identifiant et son mot de passe
- Lorsque l'utilisateur ouvre mail.chu-nantes.fr dans son navigateur, l'agent Evidian reconnaît cette adresse et saisie l'identifiant et le mot de passe de l'utilisateur dans les champs *login* et *mot de passe*

Ce mode peut être personnalisé en fonction de l'usage :

- **Mode Flash (sans contact)** : Un simple passage de la carte sur le lecteur (sans contact) déverrouille la session et lance le moteur Evidian grâce à la puce RFID de la carte
- **Mode Verrou transparent** : Lors du verrouillage de la session (après retrait carte par exemple), le bureau reste visible mais le clavier et la souris sont inopérants (utile par exemple dans le cas d'un PC d'affichage)

- **Mode Sans Verrou** : Le verrouillage de la session est inhibé mais le poste est limité fonctionnellement à une seule application (autologon, pas d'accès au bureau Windows ni à aucune application autre que celle définie à la conception) ⇒ Validation RSSI() au cas par cas
- **FUSMap Exception** : Ce mode permet d'exclure une application donnée de la liste des application a fermer lors du changement d'utilisateur et/ou de ne pas connecter les lecteurs réseaux du porteur de la carte mais de laisser ceux du compte générique

Chaque cas d'usage étant différent, la mise en place d'une solution doit être discutée avec la cellule Infra\Poste Client

Poste de travail

Plusieurs "form factors" sont mis à disposition du personnel en fonction de l'usage qui sera fait du poste de travail. Le critère principal d'affectation est généralement lié aux besoins d'affichage (taille de diagonale):

Segment	Sédentaire					Mobile		Ultramobile		Spécialisé		
Catégorie	Générique	Station	Compact			Générique	Ultra portable	Tablette	Smart phone CHU	Affichage dynamique	PDA	Vidéo projecteur
Modèle	Lenovo Think Centre	Lenovo Think Station	AllInOne	Tiny	PanelPC	Lenovo 15"	HP 13"	iPad	Surface	Android	22'	50'



Le poste de travail dispose d'un **système d'exploitation** conçu, maintenu et administré par la Direction des Services Numériques. Chaque poste de travail est qualifié en interne avant mise en production afin de vérifier sa compatibilité avec les autres éléments du SI.

Elements clef:

- Différents formats en fonction de l'usage
- Le nombre de postes a un impact fort sur d'autres coûts (Licence Microsoft, systèmes de sécurité, support...)
- L'hétérogénéité des matériels complexifie la gestion et augmente le nombre et/ou le temps de traitement des déploiement et des incidents
- Extension de la garantie constructeur (3 ou 5ans) par le titulaire du marché (jusqu'à 4ans supplémentaires)
- Chaque poste doit être qualifié et intégré aux différents systèmes par l'équipe INFRA\Poste Client
- Leur gestion est assurée par des outils dédiés (Windows avec SCCM, Apple et Android avec Microsoft Intune)
- Les mises à jour systèmes sont automatiques et obligatoire
- Acquisition auprès de marchés nationaux (CAIH, UGAP, etc.) ou hors marché (période de pénurie, demandes spécifiques, dons...)

Le matériel acquis en dehors des processus DSN() peut parfaitement être intégré au parc : Dès lors que le master CHU est installé sur le matériel, il peut être connecté au domaine CHU et bénéficier de tous les outils de gestion de configuration du CHU. Dans le cas contraire, il dispose simplement d'une connexion réseau en zone "untrusted" et le poste n'est pas géré par la DSN().

Plus d'informations ici.

Périphériques

En fonction du type de postes et de leur usage, différents périphériques sont présents sur les postes, par défaut ou en option :

Catégorie	Ecran supplémentaire	Saisie	Lecteur de Cartes	Scanner	Impressions			Dictée	Acquisition image												
Type	HD	Tablette (Quad core)	Clavier (sans fil)	Clavier 3 boutons (sans fil) (PS/2)	Gaia Sans Contact	CPU	Wi-Fi	Doublette	A plus	A la	MP3	Personnalis N&S	Personnalis Card	Papier synthétique	Thermique	Reprographie	Micro	Podcast	WebCam	Appareil photo	Caméra HD
																					

Chaque matériel doit être **référéncé** avant déploiement. Le référencement consiste à valider la capacité de la Direction des Services Numériques à acquérir, déployer, maintenir et remplacer le matériel. Le risque qu'un déploiement interfère sur d'autres composants du poste (système, logiciel, autre matériel...) doit être géré via le processus de qualification interne DSN() en amont.

Applications

Chaque application ou outil installé sur un poste CHU doit être référencé et intégré. Certaines applications\logiciels\composants sont installés en standard lors de la descente d'une image système sur un poste. Cet ensemble d'applications sont regroupés dans le socle commun aka **Master CHU**.

En fonction du résultat de la qualification initiale, le logiciel peut être déployé de différentes manières :

1. Publication d'application installée sur un serveur (Citrix XenDesktop) : L'application est installée et exécutée sur un serveur et est présentée à l'utilisateur par une technologie de déport d'affichage
2. Déploiement "Sans assistance" (MECM): L'application est préalablement packagée pour permettre une installation silencieuse et sans assistance depuis l'outil SCCM \ MECM \ ConfigMgr de Microsoft. Elle est ensuite exécutée localement.
3. Installation manuelle : L'application est installée manuellement par un technicien en suivant une procédure. Le poste est immobilisé le temps de l'installation et de la configuration.

Détail des catégories de postes

Usage prise en charge médicale du patient à destination du personnel Medico-Soignants

Les postes de type "prise en charge médicale du patient à destination du personnel Medico-Soignants" sont destinés aux médecins et/ou paraméd. Ils sont la plupart du temps partagés par plusieurs utilisateurs dans la même journée. Ils permettent de respecter les contraintes de sécurité et traçabilité par l'utilisation de la carte Gaia combinée à une configuration de type "Session partagée (kiosk)".

Poste Partagé Médico-Soignants

**Support**

Paillasse \ bureau

Mode d'Authentif.

Gaia partagé-Kiosk

Poste de travail

Fixe, Portable ou tout en un

Périphériques

- Lecteur de cartes avec contact
- Clavier avec lecteur carte intégré
- Souris
- Ecran 22 pouces

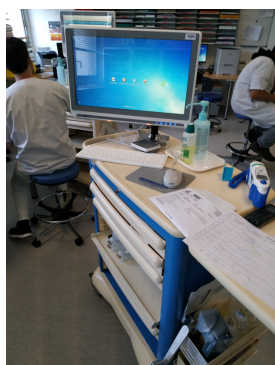
Affectation

- 1 par salle de soins
- 1 par bureau IDE
- 1 par personnel médical en salle médecins / internes / externes
- 1 par bureau de consultation

Options

- Pack lavable (clavier / souris / tapis)
- Lecteur de cartes sans contact
- Ecran 22 pouces de relecture PACS
- Pack médecin (Speechmike + suite Nuance)
- Second écran 22pouces

Distribution médicaments

**Support**

Chariot medicament

Mode d'Authentif.

Gaia partagé

Poste de travail

Autoalimenté ou poste portable

Périphériques

- Lecteur de cartes avec contact (intégré)
- Clavier avec lecteur carte intégré
- Souris
- Ecran 22 pouces

Options

- Pack lavable (clavier / souris / tapis)
- Lecteur de cartes sans contact

Affectation

- 1 par IDE en service

Chariot de visite

**Support**

Chariot de visite

Mode d'Authentif.

Gaia partagé

Poste de travail

Autoalimenté, fixe format "tiny" ou portable

Périphériques

- Lecteur de cartes avec contact
- Clavier avec lecteur carte intégré
- Souris
- Ecran 15 ou 22 pouces

Affectation

- 1 par IDE en service
- 1 par secteur pour AS
- 2 par secteur pour personnel médical

Options

- Pack lavable (clavier / souris / tapis)
- Lecteur de cartes sans contact
- Pack médecin (Speechmike + suite Nuance)

Chariots de soins

**Support**

Chariot de soins

Mode d'Authentif.

Gaia partagé-Kiosk

Poste de travail

tout en un alimenté

Périphériques

- Clavier lavable
- Lecteur carte intégré au PC
- Souris

Options

- Lecteur sans contact
- Gaia session errante

Affectation

Selon besoins \\\

Poste de consultations Médecin

**Support**

Paillasse \ bureau

Mode d'Authentif.

Gaia partagé-Kiosk

Poste de travail

Fixe, Portable ou tout en un

Périphériques

- Clavier et souris lavable
- Lecteur de cartes avec contact (x2)
- Ecran 22 pouces
- Speechmike
- Lecteur code-barre
- Imprimante

-Périphériques pour téléconsultations (En cours de qualification)

Options

- Lecteur de cartes contact\sans contact (en remplacement d'un des deux lecteurs)
- Ecran 22 pouces de relecture PACS
- Second écran 22pouces

Affectation

- 1 par bureau de consultation

Station PACS

**Support****Mode d'Authentif.**

Gaia sédentaire

Poste de travail

Station de travail au format

tour PériphériquesClavier avec lecteur carte
intégré

Souris

1 écran bureautique et 2

écrans médicaux EIZO

OptionsPack médecin (Speechmike
+ suite Nuance)**Affectation**1 station par radiologue +
stations en libre service

Usage administratif et bureautique

Portable bureautique

**Support**

Paillasse \ bureau

Mode d'Authentif.

Gaia partagé

Poste de travail

Fixe, Portable ou tout en un

Périphériques

- Lecteur de cartes avec contact
- Clavier avec lecteur carte intégré
- Souris
- Ecran 22 pouces
- Station d'accueil si portable

Options

- Second écran 22 pouces -
- Pack médecin (Speechmike
+ suite Nuance)

Affectation

- 1 par médecin
- 1 par cadre
- 1 par télétravailleur

Fixe bureautique

**Support**

Paillasse \ bureau

Mode d'Authentif.

Gaia partagé

Poste de travail

Fixe, Portable ou tout en un

Périphériques

- Clavier avec lecteur carte intégré
- Souris
- Ecran 22 pouces

Options

- Pack médecin
(Speechmike + suite
Nuance)
- Second écran 22pouces

Affectation

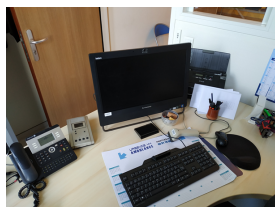
Si non équipé d'un portable :

- 1 par médecin
- 1 par cadre
- 1 par personnel adm. ou tech.

Usage Prise en charge administrative du patient

Les postes de type "Prise en charge administrative du patient" sont des postes généralement utilisés par le back office, sans contact direct avec le patient. Ce poste est généralement affecté à un utilisateur pour la durée de son service, peu d'utilisateurs se succèdent pour utiliser ces postes.

Secretariat medical (AMA)

**Support**

bureau

Mode d'Authentif.

Gaia personnel

Poste de travail

Fixe, Portable ou tout en un

Affectation

- 1 par AMA (secrétaire médicale)

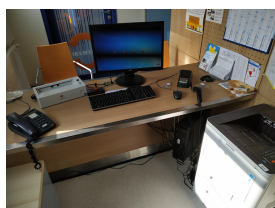
Périphériques

- Lecteur de cartes avec contact
- Clavier avec lecteur carte intégré
- Souris
- Ecran 22 pouces

Options

- Second écran 22pouces
- Scanner

Admission Guichet

**Support**

Paillasse \ bureau

Mode d'Authentif.

Gaia partagé

Poste de travail

Tout en un

Affectation

- 1 par guichet d'admission

Périphériques

- Lecteur de cartes avec contact (x2)
- Clavier avec lecteur carte intégré
- Souris
- Ecran 22 pouces
- Scanner
- Imprimante

Usage spécialisé ou technique

Bloc IBODE

Le poste de type "IBODE" est localisé en salle de bloc et est destiné à l'Infirmier.e de bloc opératoire. Il est composé d'un PC au format "tiny" installé sur un chariot de visite avec 2 écrans 22p. Un report d'écran peut être installé pour afficher le contenu du second écran vers le grand écran sur le plafonnier de bloc opératoire (écran SDI).

**Support**

Chariot

Affectation

- 1 par salle d'opération

Mode d'Authentif.

Gaia partagé

Poste de travail

Fixe ou tout en un

Périphériques

- Pack lavable (clavier / souris / tapis)
- Lecteur de cartes contact\sans contact
- Ecran 22 pouces

Options

- Scanner code barre 1D

Bloc Respirateur

Le poste de type « Blocs Respirateur» est utilisé par les médecins et infirmiers anesthésistes dans le bloc opératoire lors des interventions chirurgicales afin d'assurer le suivi de l'anesthésie à travers l'application Fusion Pégase.

Ce poste est un panel PC avec écran tactile installé sur un bras monté sur le chariot d'anesthésie.

**Support**

Chariot

Mode d'Authentif.

Gaia partagé transparent

Poste de travail

tout en un

Périphériques

- Lecteur de cartes avec contact
- Clavier avec lecteur carte intégré
- Souris

Options

- Pack lavable (clavier / souris / tapis)
- Lecteur de cartes sans contact]

Bloc SSPI

Le poste de type "Bloc SSPI" est destiné aux salles de réveil des bloc opératoires



Poste spécialisé

Même s'il dispose du Master CHU, ce type de poste répond a des contraintes lié à son usage particulier. Ces contraintes portent notamment sur la partie authentification (se référer à **la section suivante**) mais est propre a chaque projet.

Smartphone et tablettes

La DSN () peut mettre à disposition des utilisateurs et/ou des projets des périphériques de type Smartphone ou Tablettes. Ces périphériques fonctionnent sur Google Android, disposent d'un agent MDM (Gestion de terminaux mobiles Microsoft Intune) déployés selon **uniquement** deux types de configurations :

- **Configuration PRO** : Permet à l'utilisateur de disposer d'un terminal Android professionnel sur lequel la DSN () peut appliquer des politiques de sécurité, limiter l'installation d'applications, contrôler la configuration et la conformité de l'appareil tout en permettant un usage "standard" de l'appareil.
- **Configuration KIOSK** : Permet de verrouiller le terminal Android pour qu'il n'exécute qu'une ou plusieurs applications spécifiques. Il existe autant de configurations kiosk que d'usages, par exemple un terminal dédié au service brancardage ne disposera pas des mêmes applications et restrictions qu'un terminal dédié au SAMU.

Un point de vigilance doit être observé sur les restrictions sécurité et réseau des 2 types de configuration proposées (notamment réseau **TRUSTED pour KIOSK, UNTRUSTED pour PRO**) cela peut avoir un impact sur l'architecture et la solution applicative retenue

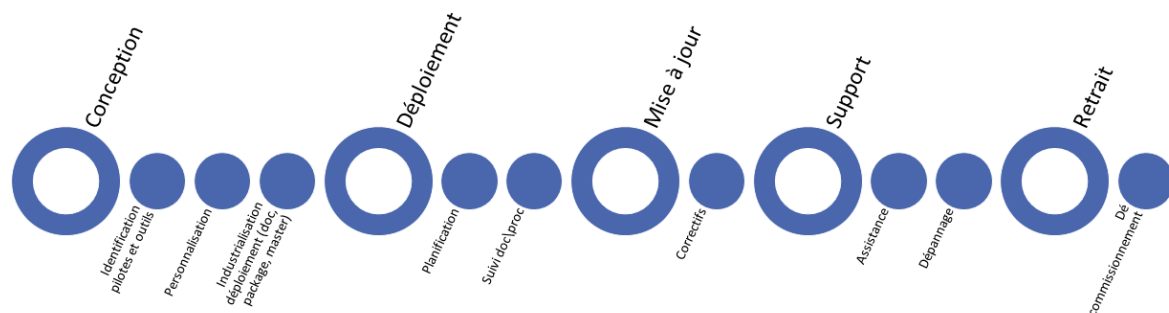
Configuration PRO	Configuration KIOSK
 Système Android à jour (Prise en charge maximum des 2 versions majeures antérieures) Interface Android "standard" (pas de restriction particulière) Appareil attribué à un utilisateur identifié (enrôlement du terminal avec son compte Microsoft Entra nominatif) Accès au Google Play Store restreint, seul les applications préalablement validées peuvent être installées Accès réseau 5G uniquement, pas d'accès wifi autre que CHU-PUBLIC	 Système Android à jour (Prise en charge maximum des 2 versions majeures antérieures) Appareil partagé, non affecté à un utilisateur identifié Usage strictement restreint à l'utilisation prévue à la conception Verrouillé sur une seule application ou un scénario métier spécifique Accès réseau 5G + accès Wifi CHUN en fonction du besoin

Normes et standards

Gestion du système d'exploitation (Windows 10)

La version de Windows 10 déployée au CHU au 01 février 2023 est la version **22H2** en version **Enterprise** et en mode **Semi Annual Channel**.

La gestion du cycle de vie du système d'exploitation suit généralement les étapes suivantes:



Conception : Saut de release Windows

Déploiement de systèmes

Mises à jour - Sécurité Microsoft (Quality

(Features Updates)

Les sauts de versions majeures suivent le découpage par cible des déploiements de correctifs Microsoft. Le déploiement précède de 6mois la date de fin de support de chaque version (<https://support.microsoft.com/fr-fr/help/13853/windows-lifecycle-fact-sheet> (<https://support.microsoft.com/fr-fr/help/13853/windows-lifecycle-fact-sheet>)). Le support de chaque release varie de 16 à 30 mois. Chaque montée de version fait l'objet d'un projet spécifique.

d'exploitation

Le déploiement de système Windows se base sur SCCM selon deux modes, **Primo** (Bare Metal OS (.) Deployment) ou **Reinstallation** (Refresh):

Primo:

1. Le poste démarre sur un media d'amorçage (Réseau via PXE ou Clef USB)
2. L'environnement de déploiement est lancé (WinPE)
3. L'infrastructure SCCM applique la séquence de tâche
4. Le nom (hostname du poste) est demandé ainsi que le déploiement à réaliser
5. L'image OS (.) (WIM) est copiée et appliquée sur la machine
6. Les applications du socle sont déployées

A l'issue de ce déploiement le poste doit être personnalisé : Le technicien, via CHUStore ("Centre logiciel" de MECM), doit sélectionner la catégorie du poste afin de déployer les applications spécifique à l'usage du poste. Les applications optionelles doivent aussi être installée via CHUStore.

Refresh:

1. Sur un systeme "Up&Running", la sequence d'installation est lancée directement depuis le centre logiciel
2. Le profil est conservé sur le disque
3. L'installation systeme est réalisée
4. Les applications précédemment installées et disponible dans le centre logiciel sont réinstallées

Les mises à jour Windows sont déployés depuis le composant Windows Software Update Services (WSUS), la recherche et l'application de mises à jour depuis Windows Updates sont désactivés.

Updates)

Le déploiement des mises à jour mensuelles est réalisé en deux temps afin de bénéficier du retour d'expérience global et limiter les effets de bord sur la compatibilité applicative :

	Date	Cible
Pilote	2eme mercredi du mois	Postes dor hostname termine pa (ex:CHU81 1000 post
Généralisation	4eme mercredi du mois	Tous les postes restants 10000 pos



Composition du socle commun (Master Windows 10)

Logiciels

La plupart des applications du socle sont mises à jour sur une base a minima trimestrielle

Ci dessous, le détail de la composition du socle commun au 01/06/2022:

Name	Vendor	Version	Commentaire	Type de MaJ
Microsoft Office 2016	Microsoft Corporation	16.0.4266.1001		Selon projets
Classic Client 6.3.5 Administrator for 64 bits	Gemalto	6.30.500.001	aka "Gaia"	Selon projets

Name	Vendor	Version	Commentaire	Type de Maj
Check Point VPN	Check Point Software Technologies Ltd.	98.61.2607	aka "MobiCHU" : Sur portable bureautique uniquement	Selon projets
Configuration Manager Client	Microsoft Corporation	5.00.9068.1000		
MDOP MBAM	Microsoft Corporation	2.5.1152.0		
Apex One	Trend Micro Inc.	14.0.11789		Selon projets
Google Chrome	Google LLC	106.0.5249.119		Maj automatique
Adobe Acrobat Reader DC - Français	Adobe Systems Incorporated	23.003.20244		
Citrix Workspace	Citrix Systems, Inc.	22.03.1000-LTSR		
Microsoft Visual C++ 2012 x86 Additional Runtime - 11.0.60610	Microsoft Corporation	11.0.60610		
SafeNet Authentication Client 10.6	Gemalto	10.6.146.0	aka "Gaia"	Selon projets
Google Legacy Browser Support	Google Inc	7.1.0.0		Maj automatique
Enterprise Access Management Client	Evidian	10.00.6846.43	aka "Gaia"	Selon projets
Nexthink Collector	Nexthink S.A.	6.29.02004	Agent Nexthink pour indicateurs sur UX	
ImageGlass	Duong Dieu Phap	8.9.6.9		
7zip	IgorPavlov	23.01		
VLC	VideoLAN	3.0.18		

Taches de maintenances et remise en conformité

Des contrôles de conformités sont réalisées de façon récurrentes et généralement automatisées pour conserver une homogénéités des configurations. Le détail des opérations est listé dans le tableau ci dessous :

Cible	Contrôle	Conformité sccm	Opérations réaliser	Procédure de contrôle et remédiation
Conformité Windows	Il ne doit pas y avoir de fichiers avec une date de création de + de 90 j dans les répertoires: "C:\Windows\ccmcache" "C:\Windows\temp" "C:\Users*\AppData\Local\Temp" Purge des fichiers temporaire Qbloc Retrait des appx non nécessaire Correction WinRM	BL_Windows_Maintenance	CI_O_PurgeSCCM, CI_O_FichierTemp, CI_U_FichierTemp, CI_Qbloc_FichierTemp, CI_O_WindowsAppx, CI_O_Windows_WinRM	Correction automatique par la Baseline
Conformité Crowstrike	Présence de l'agent Crowdstrike sur le poste de travail	BL_CrowdStrike	CI_CrowdStrike_Présence	Pas de correction automatique
	Présence du service de CrowStrike	BL_CrowdStrike	CI_CrowdStrike_Service	
Conformité Citrix	Présence de Worspace one si c'est un poste sédentaire			
Conformité Chrome	Derniere version de Chrome	BL_GoogleChrome	CI_O_ChromeVersion	
	Cache moins d'une journée		Vidage cache Chrome tous les jours (lenteurs intranet)	
	Suppression du coffre fort chrome	BL_GoogleChrome	CI_U_GoogleChrome_CoffreFort	

				Procédure de contrôle et remédiation
Cible	Contrôle	Conformité sccm	Opérations réaliser	
	Présence des KB du mois précédent			
Conformité Sccm	Etat de santé de l'agent Sccm	BL-AgentSCCM	CI_O_SantéAgentSccm	
	Si le groupe local "ConfigMgr Remote Control Users" existe, le groupe local "Utilisateurs du contrôle à distance ConfigMgr" ne doit pas exister	BL-AgentSCCM	CI_O_GrpPriseDeMains	
Conformité Gaia	Présence de la dernière version Gaia	BL-PostesGaiaKiosk / BL-PostesGaiaSedentaire	CI_O_ConfigGaia-SSO-Engine_Up2date	Intégration dans un groupement sccm pour exécutions manuelle de la maj
	Nettoyage fichiers de log	BL-PostesGaiaKiosk / BL-PostesGaiaSedentaire	CI_O_GaiaPurgeLog	
Conformité Kit de survi	Kit de survie a jour	BL_KitDeSurvie	CI_KitDeSurvie_PrésenceDate	
Conformité Microsoft office	Presence de Office 2016 std x64 ou pro x64 - Non conformité si presence de std ET pro - Non conformité si présence autre version Office	BL-Office2016x64		
Tous les postes de travail	Si le poste est présent dans AD, il doit etre en statut "en fonction" dans EZV Si le poste est en fonction dans EZV, il doit etre présent dans AD Si le poste est dans AD, il doit etre dans SCCM		Désactivation des postes de travail dans l'AD par script hebdomadaire si il ne repsecte pas l'un des critères	
	Présence des KB du mois précédent			
Tous les Ultraportable	Vérification de la version du client vpn checkpoint	BL-MobiCHU-Checkpoint-MAJ	CI_O_Checkpoint_v84.60	
Tous les PC Win7	Présence du WMF 5.1	BL-WMF5.1Presence	CI_O_FrameworkK5.1-Presence	
Tous les kiosk	FUSMap à jour	BL-PostesGaiaKiosk	CI_O_ConfigGaia-CopieFUSMapNetworkDrive	
	Appartenance a un seul groupe AD FUSxxxx	BL-PostesGaiaKiosk	CI_O_GrpFusPrésence	
	Absence de MobiCHU	BL-PostesGaiaKiosk	CI_O_CheckpointNotExist	
	Vérification autologon	BL-PostesGaiaKiosk	CI_O_ConfigGaia-AutologonExist	
Tous les sédentaires	Absence de FUSMap	BL-PostesGaiaSedentaire	CI_O_ConfigGaia-FUSMapPrésence	
	Absence d'autologon	BL-PostesGaiaSedentaire	CI_O_ConfigGaia-SansAutoLogonUserLogin	
	Présence du fichier Sédentaire identité	BL-PostesGaiaSedentaire	CI_O_Checkpoint_PresenceSedentaireIdentite	
Postes secours		BL-PosteSecoursIcca	CI-ConfigPosteSecours-Icca/CI-ConfigPosteSecours-CompteLocalSecours	Correction automatique par la Baseline

Cible	Contrôle	Conformité sccm	Opérations réaliser	Procédure de contrôle et remédiation
		BL-PosteSecours724	CI-ConfigPosteSecours-724/CI-ConfigPosteSecours-CompteLocalSecours	Correction automatique par la Baseline
		BL-PosteSecoursEasily	CI-ConfigPosteSecours-Easily/CI-ConfigPosteSecours-CompteLocalSecours	Correction automatique par la Baseline

Outils d'administration

Prise de main à distance

Gestion des postes client Microsoft

Les postes clients sont gérés par l'outil Microsoft Configuration Manager (v2303). Cet outil est utilisé pour répondre aux usages suivants:

- Déploiement de systèmes d'exploitation Windows 10 et Windows 11
- Déploiement des mises à jour système Microsoft
- Déploiement de packages applicatif
- Prise de contrôle à distance
- Inventaire matériel et logiciel
- Gestion de conformité (Analyse et/ou correction)

Gestion des terminaux Android

Certains terminaux Android sont gérés via installation d'un agent Microsoft Intune. Cet outil est utilisé quasi exclusivement à limiter l'accès de l'utilisateur à une ou plusieurs applications spécifiques, empêchant ainsi l'utilisation non autorisée d'autres fonctionnalités ou applications de l'appareil.

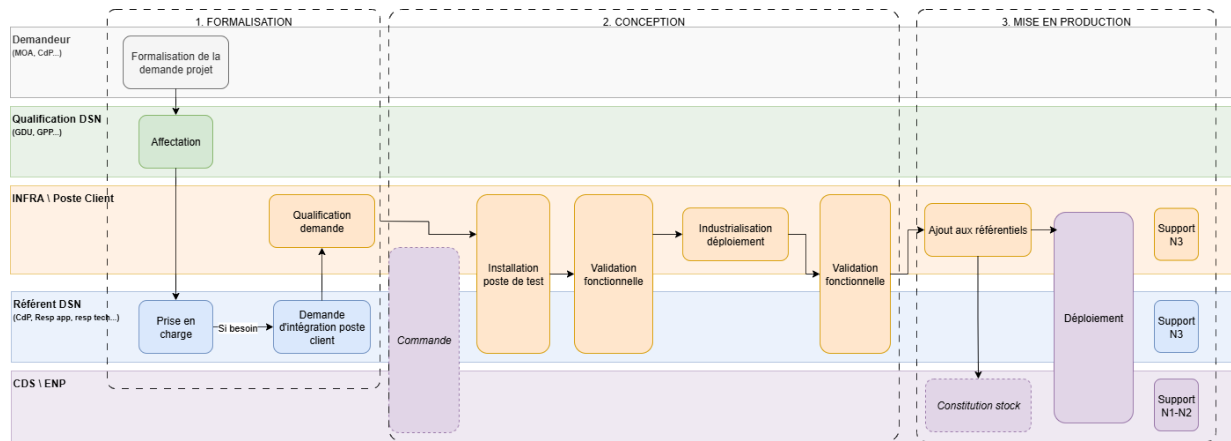
Principe de gestion des nouvelles références (nouveau logiciel ou nouveau matériel)

Toute application et matériel présent sur le parc informatique doit être identifié et documenté préalablement au déploiement en production.

L'objectif est principalement de maîtriser l'hétérogénéité des matériels ou logiciels de marque/modèle différents pour un même usage. Cette homogénéité des références réduit la complexité de gestion (acquisition, constitution de stocks, qualification, déploiement, dépannage, maintenance, remplacement...).

L'ajout de nouveau matériel ou logiciel client n'est généralement qu'une activité parmi d'autres dans le cadre d'un projet d'intégration ou de mise à jour applicative : L'intégration d'une application métier implique plusieurs changements ou activités (ex: création des VM serveurs, installation configuration des BDD, gestion des flux réseaux ...) et la prise en charge de la partie "poste clients" est l'une d'elle.

Les principales étapes de cette intégration coté "poste client" est précisée dans le schémas ci dessous:

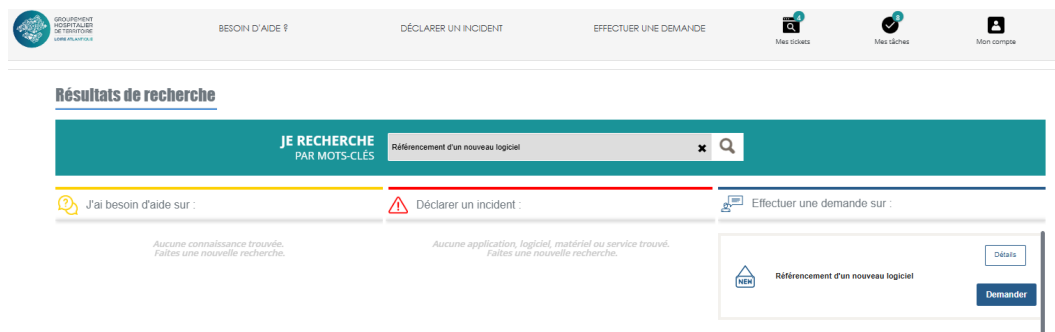


Détail Etape 1 : Formalisation

Demande de référencement \demande de projet

La point de départ d'une nouvelle intégration peut passer par une "demande de référencement" ou plus généralement par le processus standard de gestion de projet (GPP).

La "demande de référencement" est généralement directement émise par la MOA et permet d'officialiser une demande de prise en charge par la DSN () d'un besoin non couvert par les items existant au catalogue. Cette demande doit être formalisée depuis l'outil d'ITSM Easyvista:



L'équipe Gestion des Demandes Unitaires (GDU) vérifie la cohérence de la demande et l'affecte pour analyse à l'équipe DSN () la plus à même d'y répondre. Suite à cette qualification, la demande suit le processus habituel GPP.

Demande d'integration de logiciel ou matériel

Dans le cadre du processus GPP, si le projet nécessite l'ajout au parc d'un matériel ou d'un logiciel client non référencé, le chef de projet réalise une "demande d'integration de logiciel" ou une demande "référencement matériel" en fonction du besoin.

Principales étapes de l'intégration:

1. Le Responsable d'Application (RA) fait une demande d'intégration à infra\PC dans l'ITSM EasyVista
2. Un atelier avec le RA est organisé par infra\PC pour installer l'application sur un device « vierge »
3. Le RA valide le fonctionnement de l'appli sur le device de test (avec ou sans sa MOA)
4. Après cette validation, infra\PC travaille sur l'industrialisation du déploiement (doc d'install wiki, package SCCM, publication Citrix, integration MDM...)
5. Dans le cas d'un package SCCM, d'un profil MDM ou publication Citrix, le RA et/ou la MOA valide cette solution industrialisée sur un poste (l'objectif est notamment de s'assurer qu'il n'y ai pas de régression entre l'installation manuelle et l'installation auto)

6. Après cette phase, l'appli est officiellement en prod et peut être déployée par les équipes CDS

Intégration de logiciel DSN.()

Référencement de materiel DSN.()

L'intégration d'un nouveau logiciel client sur un PC CHU de Nantes suit les étapes définies dans le workflow "Demande de service / Back Office / DSN.() application / Integration de logiciels DSN.()"

Le référencement d'un nouveau materiel au parc CHU de Nantes suit les étapes définies dans le workflow "Demande de service / Back Office / DSN.() materiel / Referencement materiel DSN.()"

Le formulaire permet d'identifier et formaliser le périmètre (Nombres d'utilisateurs cible, dépendance avec le(s) logiciel(s)...)

Le formulaire permet d'identifier et formaliser le périmètre (Nombres d'utilisateurs, fréquence d'usage, profiles, mode d'accès, dépendance avec le matériel, licences, mode d'authentification...)

Détail Etape 2 : Conception

Cette étape répond à plusieurs objectifs:

- En se basant sur la documentation éditeur ou intégrateur, vérifier que l'installation est possible dans le contexte CHU, identifier les adaptations éventuelles (changement de versions de composants, exclusion AV...)
- Pour un materiel, valider qu'il n'impact pas d'autres éléments et qu'il est compatible avec les équipements ou les logiciels existants
- Réaliser et valider l'intégration avec le demandeur (Réfèrent applicatif et/ou réfèrent technique)
- Choisir le mode de déploiement (Publication avec Citrix, déploiement automatisée avec MECM (ciblage utilisateur ou machine), installation manuelle sur procédures...)
- Configuration de la publication \ Conception du package \ rédaction documentation
- Validation/recette par le demandeur via tests applicatifs \ fonctionnels pour s'assurer que le mode de déploiement sélectionné ne crée pas de régression par rapport aux tests précédents

La mise à disposition \ installation d'une application sera réalisée via les technologies suivantes (voir ici pour la description) :

1. Mode publication d'application (Citrix XenApp)
2. Mode installation traditionnelle (MSI, InstallShield...) sans assistance (unattended) via CHUStore
3. Mode manuel interactif

Le tableau ci-dessous synthétise les principaux critères de choix :



CRITERES FONCTIONNELS

L'application doit cibler des ordinateurs précis et non des utilisateurs	non	oui	oui
L'application doit être accessible par les utilisateurs ciblés (et uniquement ceux-ci) sur les postes partagés (type kiosk)	oui	non	non
L'application dépend d'un matériel	non	oui	oui
La documentation d'installation\paramétrage n'est pas fournie et des choix différents doivent être réalisés en fonction de l'utilisateur ou du poste cible	non	non	oui
L'application doit "suivre" l'utilisateur , quel que soit son poste (roaming de sessions)	oui	non	non
L'éditeur ne valide pas une utilisation Citrix	non	oui	oui
Mise à jour fréquente	oui	non	non
Le périmètre est tres limité (peu d'utilisateurs et/ou de postes)	oui	non	oui

CRITERES TECHNIQUES

L'application est proche du système (installation de pilotes ou services)	oui	oui	oui
Forte contraintes réseaux (latence, débit...) ⇒ Utilisable en VPN ADSL?	oui	non	non
L'application n'est pas installable en mode silencieux sans assistance	oui	non	oui

Détail Etape 3 : Mise en production

Cette étape consiste à réaliser les actions nécessaire à un passage en production du nouvel actif (CI) :

- Rédaction de la documentation Wiki (installation, dépannage, maintenance, consommable éventuels), création du CI EasyVista, référencement dans MECM
- Validation des éléments nécessaires au passage du Build au Run (support, maintenance, évolutions...) par le CdS
- Déploiement en production (pilote puis généralisation) selon séquençement et organisation définit avec le CdP

Connexion d'un équipement au réseau CHU (Fourniture par société externe)

Politique de sécurité

Un matériel est considéré comme "extérieur" dès lors qu'il ne dispose pas du socle et des composants validés et supportés par la DSN(.) du CHU (Pour un PC, le "Master CHU" windows). Il n'est pas référencé dans l'ITSM (sauf si achat DSN(.)), pas présent dans l'Active Directory et ne dispose pas de l'agent MECM\SCCM et ne dispose d'aucun logiciel DSN(.).

Dans le cas d'une nécessité de connexion d'un équipement extérieur au réseau interne du CHU, une justification doit être formalisée et approuvée par le RSSI(). Les SN du CHU de Nantes se réservent la possibilité de proposer que l'acquisition projetée soit prise en charge dans le cadre d'un de ses marchés. Une demande ne pourra être approuvée sans respect des contraintes suivantes (source PSI SMSI SOA Doc PTS) :

A13 - Sécurité des communications
Gestion de la sécurité des réseaux
Les réseaux sont cloisonnés.

Les équipements informatiques (PC, MFP, équipements biomédicaux) sont déployés dans la version OS et patch officielle de la DSN, disposent d'un MASTER DSN avec le pack des outils (SCCM, intégration AD, AV à jour, PDM, GA IA, etc.) et sont intégrés au domaine AD et gérés de façon industrielle avec le reste du parc.

Les équipements qui ne peuvent pas respecter cette configuration sont isolés sur des VLAN filtrés derrière un pare-feu interne, il appartient au demandeur de fournir la liste des flux et des IP.

Toute exception à cette règle et toute modification du MASTER doit être explicitement validée par le RSSI.

Le VLAN des admins est isolé.

Types de réseaux disponible

Deux types de réseaux sont disponibles pour connecter un équipement au réseau CHU:

Réseau Bureautique (Zone de confiance, réseau "TRUSTED")

Réseau Isolé (Zone non fiable, réseau "UNTRUSTED")

Types d'accès:

- Accès aux ressources internes (intranet) sans restriction
- Accès aux ressources externes (internet) selon PSSI
- Connexion Ethernet\Filaire (intra.chu-nantes.fr) ou WLAN\Sans-fil (Wi-Fi avec authentification 802.1x par certificats au CHU-MEDICAL)
- Accès complet au réseau UNTRUSTED (Un actif du réseau TRUSTED peut accéder sans restriction au réseau UNTRUSTED)

Contraintes:

- **Si Windows, réinstallation obligatoire du poste avec le master CHU Windows**
- **Si matériel Android, installation obligatoire de l'agent MDM (Accès "kiosk", restreint aux applications autorisées)**
- Présence des mises à jour de sécurité système Microsoft (KB) et composants tiers (Framework, navigateurs, utilitaires...) à M+1 max
- Présence de l'antivirus/EDR à jour

Types d'accès:

- Service d'échanges de fichiers (depuis *Untrusted* vers *Trusted* ou depuis *Trusted* vers *Untrusted*) offert par une passerelle gérée par la DSN() du CHU (Geodrive)
- Accès aux ressources internes (intranet) **sur liste uniquement** et soumise à validation RSSI()
- Accès aux ressources externes (internet) **sur liste uniquement** et soumise à validation RSSI()

Contraintes:

- Système d'exploitation géré par l'intégrateur (acquisition, installation, configuration, maintenance)
- Tout les flux réseaux sont fermés sauf ceux explicitement listés dans la matrice de flux
- Aucun outil/logiciel/application CHU n'est présent sur le poste
- La DSN() ne propose pas de support en dehors des accords négociés lors de la connexion de l'équipement
- **Pas de connexion Wifi autre que CHU-PUBLIC (accès internet seulement)**

Exigences pour l'intégrateur:

- Fourniture de la matrice de flux réseau (port\protocole\source\destination)
- Obligation de mise à jour régulière du système et des applications
- Formalisation de la méthode de prise de main
- Obligation de présence d'un antivirus avec mise à jour régulière

Gestion de la conformité

L'objectif de la gestion de conformité est d'**assurer la conformité des configurations avec le référentiel** (version système, composants du socle, correctifs, composants de sécurité, référencement des actifs...).

La visibilité globale de la conformité est basé sur la consolidation d'informations provenant de plusieurs outils et référentiels (Active Directory, NMap, Trend, SCCM...).

La remise en conformité s'appuie principalement sur l'outil Microsoft System Center Configuration Manager (SCCM) en version Current Branch (au 15 janvier 2019 : version 1802, version du Site 5.0.8634.1000)

Referentiel documentaire des applications DSNT
