Systancia

the human face of the workplace

SYSTANCIA GATE
Manuel utilisateur

#Cybersecurity #Virtualization #AI

www.**systancia**.com

Réf.:	FR_GATE_MA-0002_rev.2.08_Manuel utilisateur - Systancia Gate.docx
Version :	2.08
Produit :	Systancia Gate
Date :	2022-03-15

Objet :

Ce manuel a pour but d'orienter les utilisateurs dans l'utilisation de Systancia Gate.

L'utilisateur s'authentifie et aux regards de ses droits, la plateforme de Médiation lui présente les ressources qui lui sont accessibles. L'utilisateur peut activer une ressource afin d'accéder à son application de manière sécurisée.

TABLE DES MATIERES

1. Préambule

L'accès au portail Systancia Gate vous permet d'accéder à des ressources mises à disposition par votre administrateur.

Certaines de ces ressources nécessitent l'installation de composants particuliers sur le poste utilisateur. Les ressources en question sont reconnaissables au fait qu'elles fassent appel à un plugin.

Vous trouverez dans cette documentation les informations nécessaires concernant l'installation de ces composants, en fonction du système d'exploitation utilisé.

2. Règles pare-feu

Lors de l'utilisation du client Gate l'utilisation de ressources nécessitant ces utilitaires est soumise à une connexion vers le serveur Gate Mediation sur une adresse et un port spécifique.

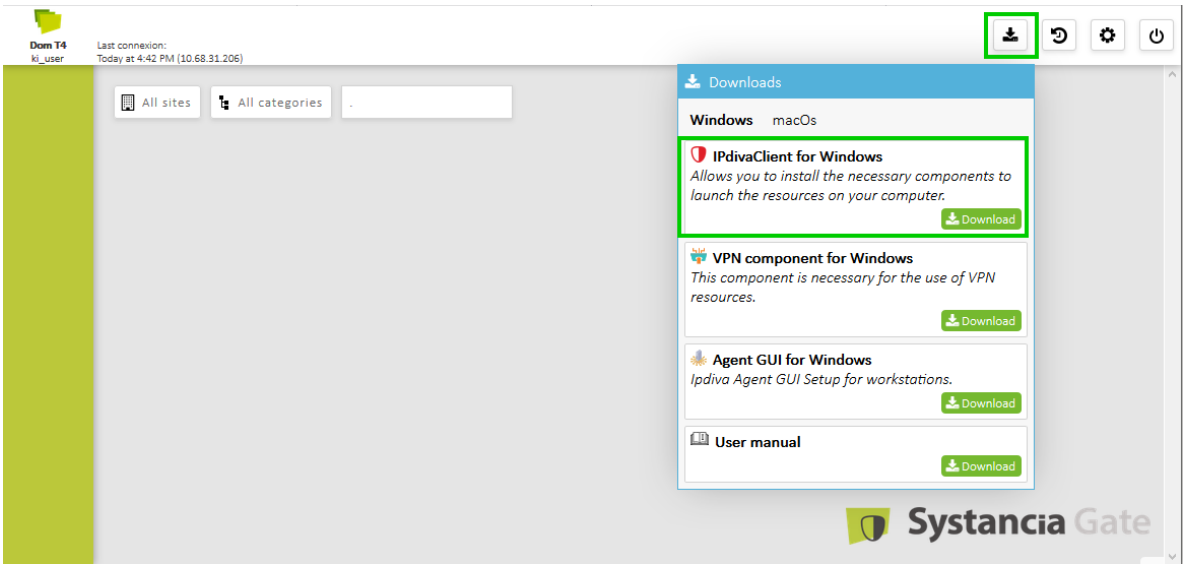
La configuration étant définie par votre administrateur, veuillez le contacter afin qu'il vous informe sur l'adresse et le port à autoriser pour la connexion des plugins.

3. Installation des clients Systancia Gate

3.1 Client Gate et Client VPN

L'installation du client Gate se fait au moyen d'un package à exécuter sur le poste utilisateur. Ce dernier peut être récupéré depuis le menu « **Téléchargement** » lorsque vous êtes connectés sur le portail Systancia Gate.

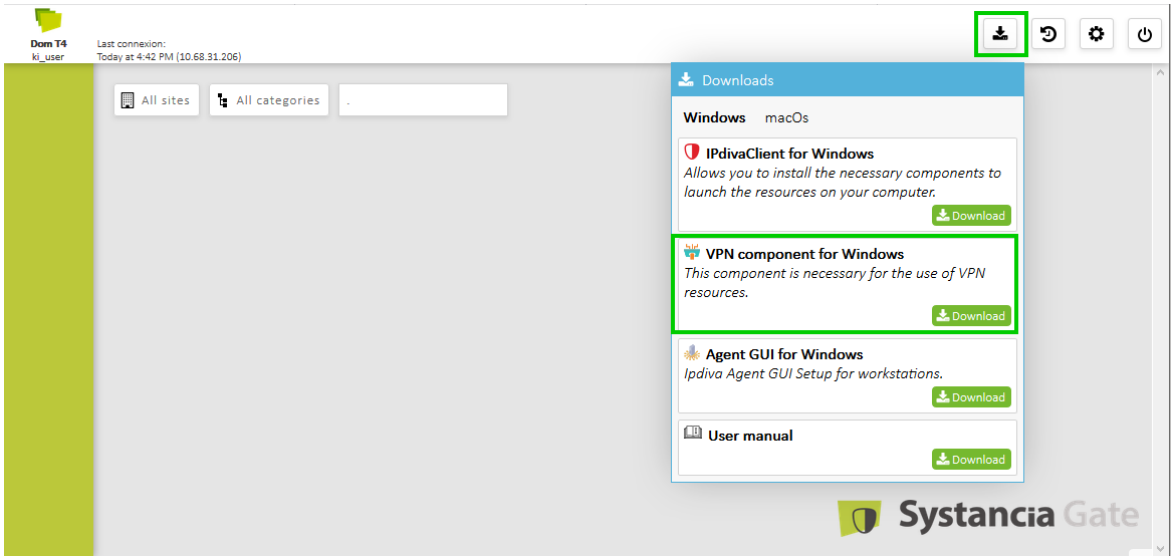
Si l'onglet est absent, il sera nécessaire de vous rapprocher de l'administrateur en charge de la solution.



L'installation du client ne nécessite aucune configuration particulière. Une fois celui-ci installé il est possible de lancer des ressources depuis le portail utilisateur.

Lors de l'exécution d'une ressource, le client apparait dans la systray :

En complément, si vous devez accéder à des ressources de type VPN, il est nécessaire d'installer le client VPN sur le poste utilisateur. Ce dernier peut être récupéré au même endroit que le client Gate.



L'installation ne demande aucune configuration particulière.

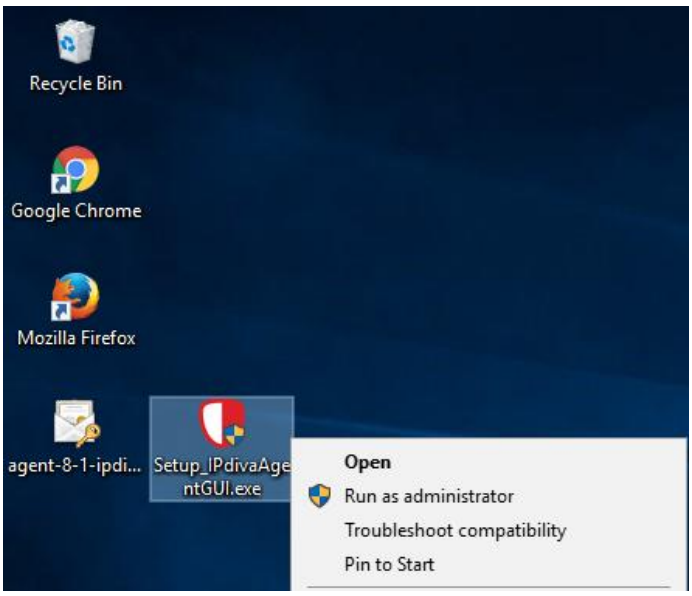
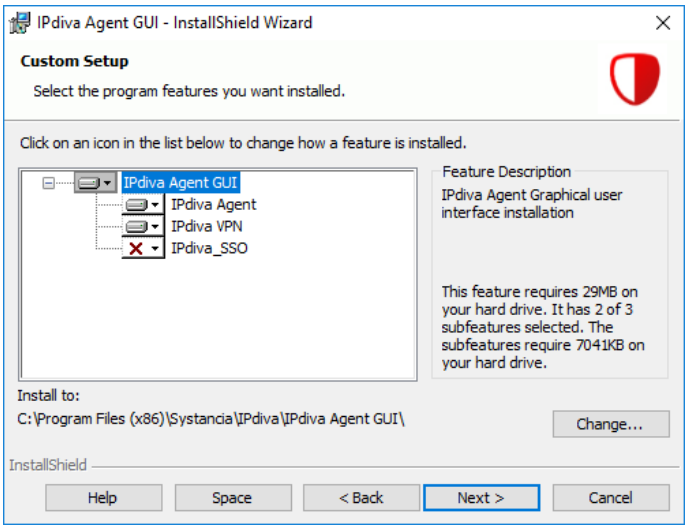
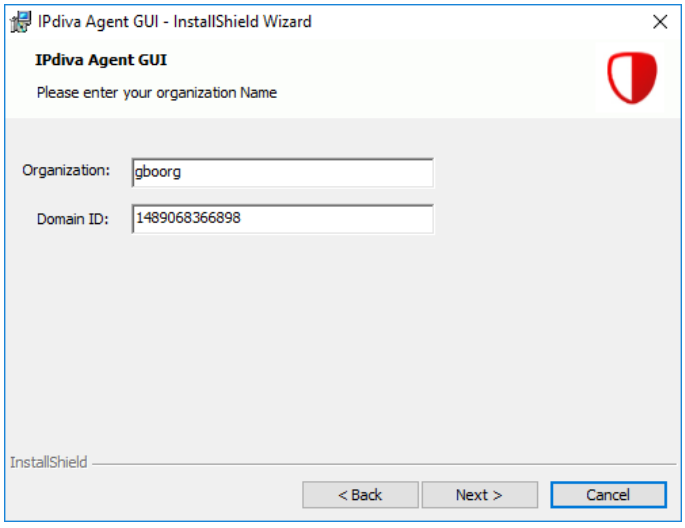
3.2 Utilitaire AgentGUI

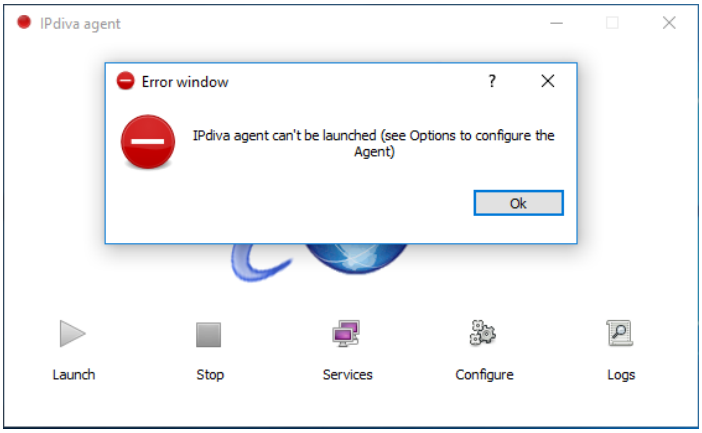
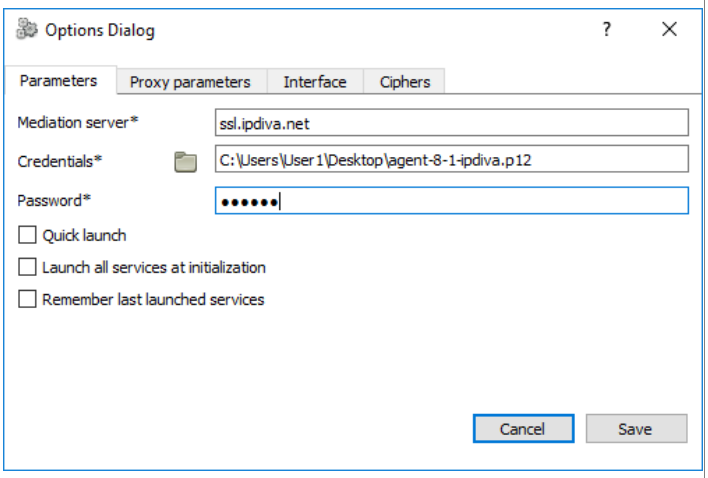
Systancia Gate propose un utilitaire supplémentaire **IPdivaAgentGUI** pour l'utilisation de ressource VPN et redirections de ports uniquement via une interface graphique dédiée.

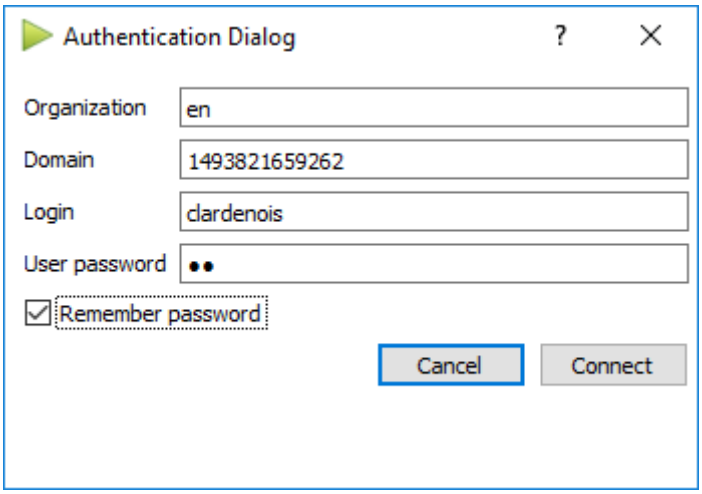
L'agent GUI permet de pouvoir lancer une ressource « **VPN** » ou plusieurs ressources « **redirection de ports** » sur le poste utilisateur sans passer par le navigateur.

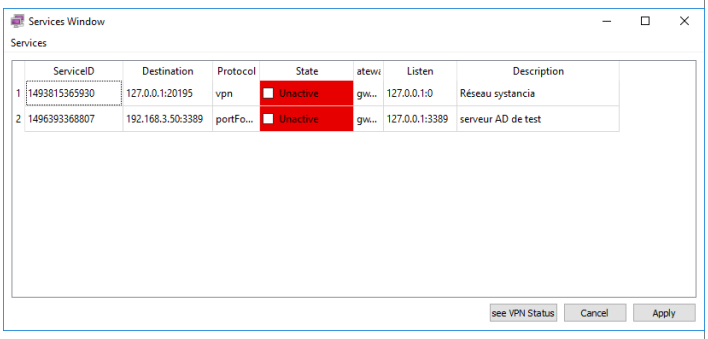
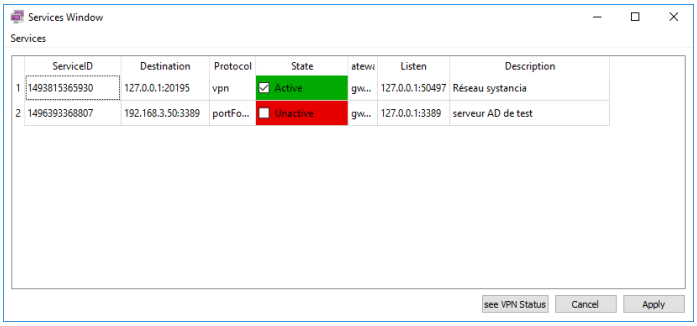
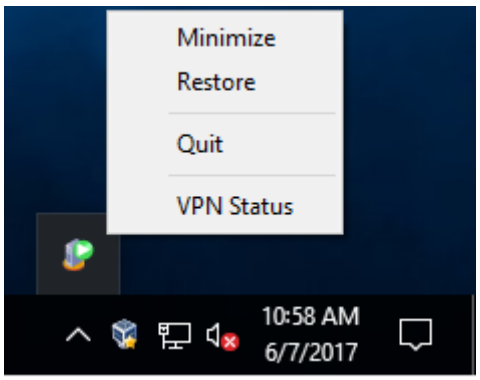
Pour utiliser l'agent GUI, il est nécessaire, en plus du programme d'installation, de disposer d'un certificat au format «.p12 ». Il est conseillé de se rapprocher de l'administrateur en charge de Systancia Gate pour obtenir ce dit certificat.

Vous trouverez ci-dessous les étapes d'installation et de configuration de l'agent GUI.

Captures d'écran	Commentaires
	Exécutez le programme d'installation de l'agent GUI avec les droits d'utilisateur privilégié (clic droit sur l'exécutable => « **Exécuter en tant qu'administrateur** »).
	Vérifiez que les composants « **IPdiva Agent »** et « **IPdiva VPN** » seront bien installés (comme l'image ci-contre) puis cliquez sur « Next ».
	Renseignez le nom de l'organisation ainsi que l'identifiant unique de l'annuaire sur lequel l'agent GUI doit se connecter puis cliquez sur « **Next** ». **Si vous ne disposez pas de ces informations, il vous sera nécessaire de vous rapprocher de l'administrateur de la solution Systancia Gate.* *Vous pouvez quand même cliquer sur « **Next** » pour poursuivre l'installation.*

Captures d'écran	Commentaires
	Au premier lancement de l'agent GUI, une erreur apparaît car l'agent n'est pas configuré. 1 - Cliquez sur « **OK** ». 2 - Cliquez sur « **Configurer** ».
	Dans la fenêtre de configuration de l'agent, remplissez les champs suivants : **Serveur de médiation :** Saisir l'adresse (nom ou adresse IP) + port (si différent de 443) du routeur SSL IPdiva. **Certificat :** Sélectionnez le chemin où se trouve le certificat de l'agent. **Mot de passe :** Renseignez le mot de passe associé au certificat. Une fois terminé, cliquez sur « **Enregistrer** » pour sauvegarder la configuration. ***Options facultatives :*** **Lancement rapide :** Cocher la case pour que l'agent se connecte automatiquement au démarrage de ce dernier. **Lancer tous les services au démarrage :** Cochez la case pour lancer tous les services associés à votre compte utilisateur. **Se souvenir des derniers services lancés :** Cochez la case pour lancer le(s) dernier(s) service(s) utilisés au prochain lancement de l'agent.

Captures d'écran	Commentaires
	Une fois configuré, cliquez sur l'icône « **Lancer** » (encadré ci-contre) pour initier le démarrage de l'agent.
	Une nouvelle fenêtre vous demandant de renseigner plusieurs informations apparait, il est nécessaire de remplir tous les champs. **Organisation* :** Renseignez le nom de l'organisation IPdiva. **Domaine* :** Renseignez l'identifiant unique de l'annuaire sur lequel l'agent IPdiva doit se connecter. **Login :** Renseignez votre identifiant utilisateur de connexion **Mot de passe :** Renseignez le mot de passe associé à l'identifiant indiqué précédemment. *Si vous ne disposez pas de ces informations, il vous sera nécessaire de vous rapprocher de l'administrateur de la solution IPdiva.
	Si toute les informations ont bien étés renseignées et que l'accès fonctionne, le rond situé à en haut à gauche à côté d' « **Agent IPdiva** » doit être vert (*1*). De même, l'icône « **Lancer** » doit être grisée. Si la case « **lancer tous les services** » n'a pas été sélectionné précédemment, cliquez sur « **Services** » (2).

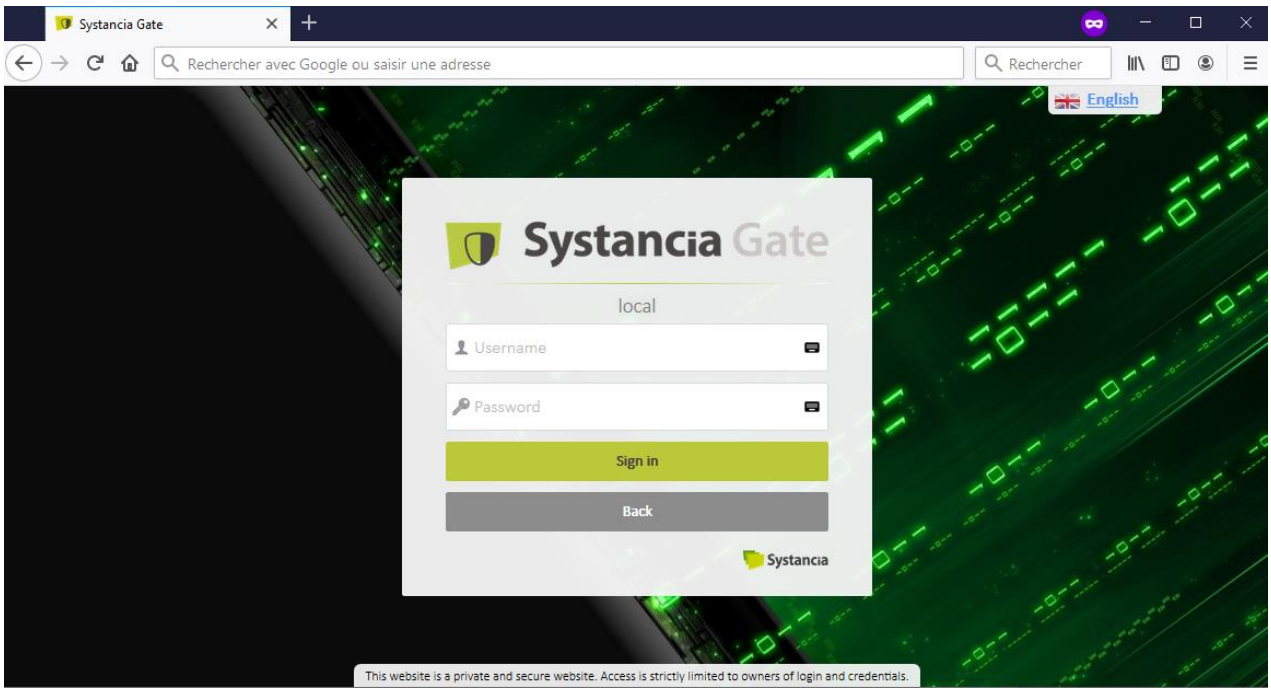
Captures d'écran	Commentaires
	Dans la nouvelle fenêtre apparue, sélectionnez le(s) service(s) à activer dans la colonne « **Etat** ». Une fois les services sélectionnés, cliquez sur « **Appliquer** »
	Le service devient alors actif et la colonne « **Etat** » devient vert. Vous pouvez dès à présent accéder à l'équipement distant. Vous pouvez alors quitter la fenêtre en cliquant sur « **Annuler** » puis fermer l'interface de l'agent GUI afin qu'il soit réduit dans la barre des tâches de Windows.
	Si vous souhaitez quitter définitivement le programme, faire un clic droit sur l'icône de l'agent GUI puis sur « **Quitter** ».

4. Connexion au portail d'accès

4.1 Page d'accueil

A partir du navigateur se connecter au portail d'accueil situé à une URL de type :

https://gate.mycompany.net/gate/cloud

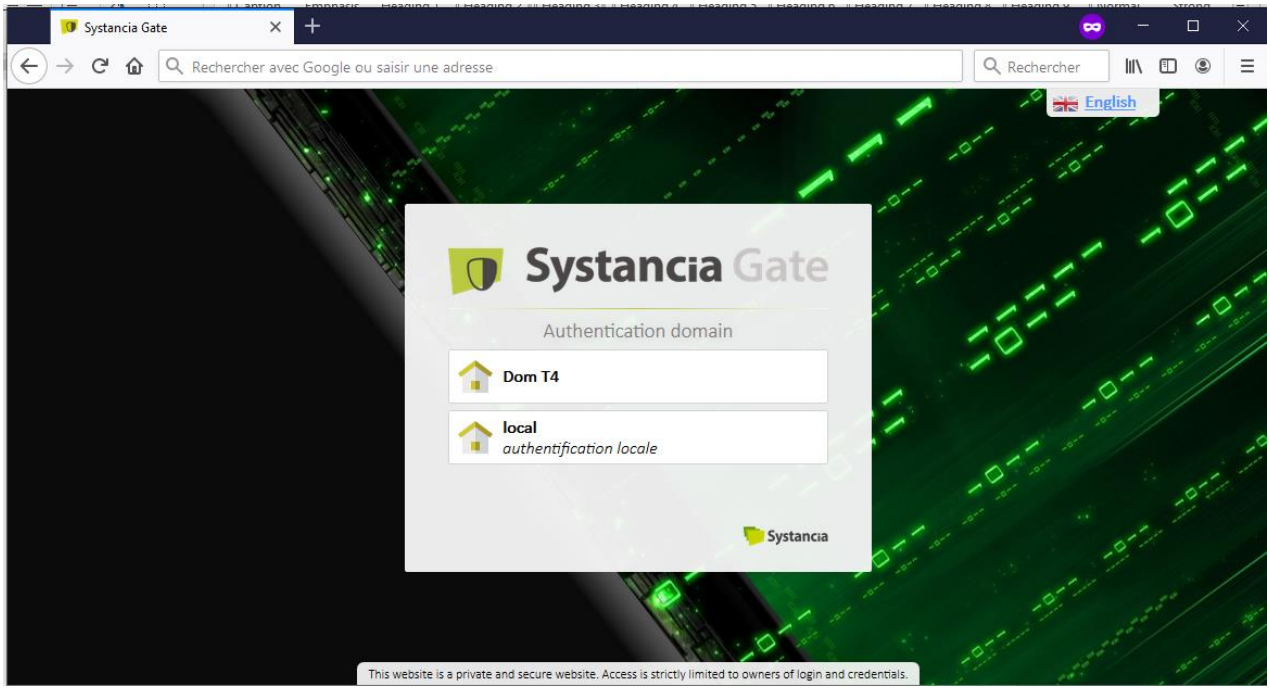


Note 1 : En cas **d'authentification mutuelle par certificat X509**, le navigateur vous propose aussi une fenêtre de sélection d'un certificat utilisateur présent sur le poste que vous utilisez (uniquement dans le mode de sélection manuelle configurable au niveau du navigateur. Dans le cas contraire, le certificat est automatiquement transmis). La présence ou l'absence de ce certificat conduira à des restrictions d'accès voire à l'interdiction d'accès à la plateforme et aux services rendus.

4.1.1 Choix du domaine d'authentification

En fonction du paramétrage de la solution d'accès, il est possible que vous ayez à choisir le domaine sur lequel vous allez vous authentifier en préambule à cette authentification. Vous devrez avoir reçu les instructions de votre administrateur quant à la sélection de ce domaine pour votre profil.

La page ci-dessous donne un exemple de ce type de présentation.

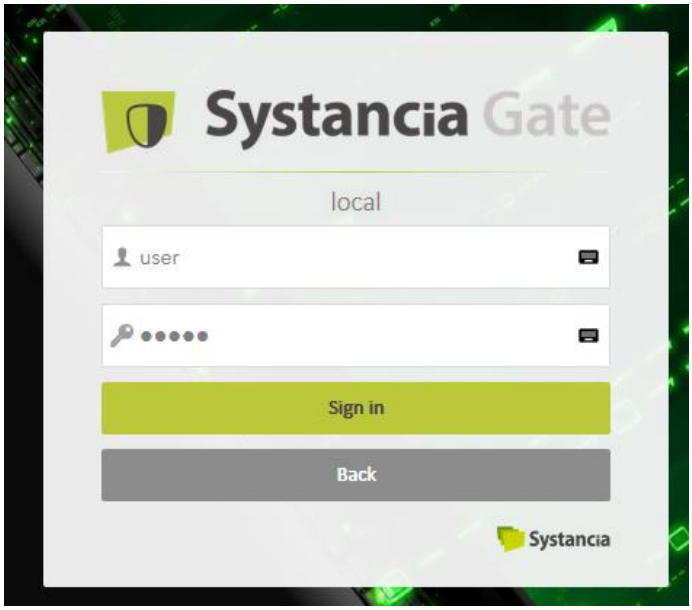


4.1.2 Identification et authentification

Il existe 3 types de formulaire d'authentification :

4.1.2.1 Authentification standard

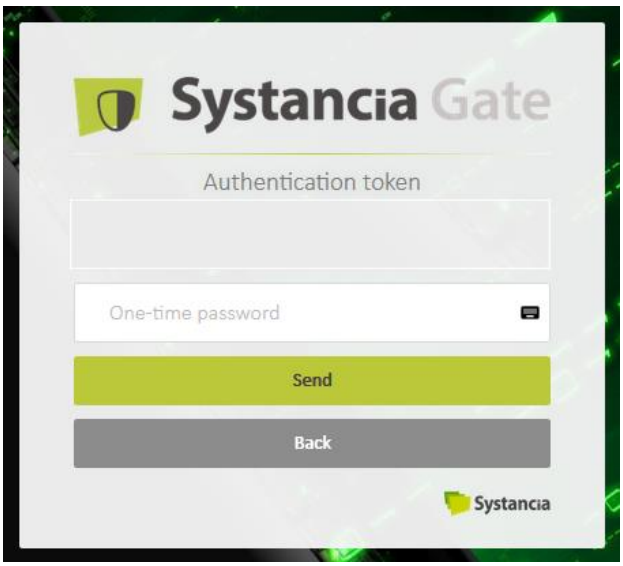
L'authentification sur le portail Systancia Gate se fait via la saisie d'un identifiant ainsi que d'un mot de passe.



4.1.2.2 Authentification forte

A la différence d'une authentification standard, lorsque vous cliquez sur le bouton « **Valider** » pour vous authentifier, champ supplémentaire apparaitra vous demandant de renseigner un mot de passe à usage unique.

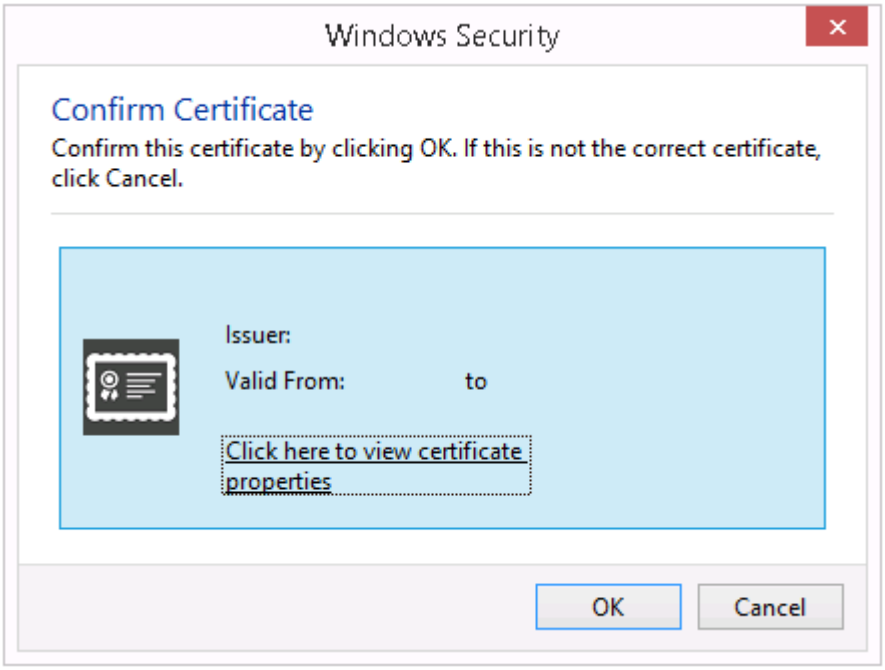
Suivant la configuration mise en place par votre administrateur, le mot de passe unique peut être reçu par mail ou par sms ou généré via une application mobile



4.1.2.3 Authentification par certificat / carte CPS

Ce mécanisme d'authentification fonctionne en deux étapes.

Lorsque vous tentez d'accéder au portail Gate, il vous est demandé (par défaut dans la configuration des navigateurs) de sélectionner le certificat / carte CPS à utiliser pour accéder au portail.



Une fois validé, suivant la configuration mise en place par l'administrateur, vous pourrez accéder aux ressources ou alors il vous sera demandé de renseigner un identifiant (ce paramètre pourra être pré-rempli suivant la configuration) + mot de passe.

4.1.3 Contrôles d'intégrité et de conformité

Suite à votre authentification, des contrôles additionnels sur votre environnement de connexion pourront être exigés. Un message spécifique vous avertira de l'exécution de ces contrôles.

Si le résultat de ceux-ci n'est pas conforme aux exigences attendues, votre connexion sera rejetée ou pourra faire l'objet de restrictions.

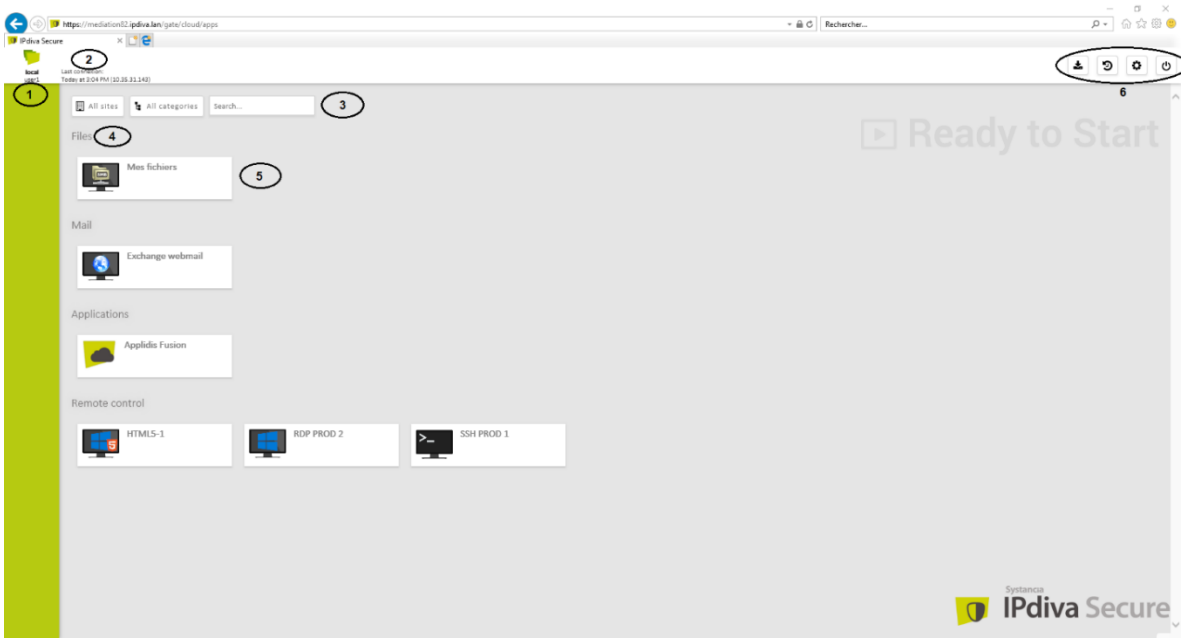
La configuration de ces contrôles et la politique à suivre en cas de non-conformité à tout ou partie de ces contrôles est du ressort de l'administrateur de la solution d'accès.

4.2 Interface utilisateur

4.2.1 Présentation des ressources

Par défaut, lorsque l'utilisateur valide l'authentification sur Systancia Gate, il accède à l'onglet des ressources. En fonction des droits qui ont été conférés à l'utilisateur par l'administrateur de la solution, une liste de ressources est proposée.

Vous trouverez ci-dessous une présentation globale de l'interface avec le positionnement des différents éléments mis à disposition.



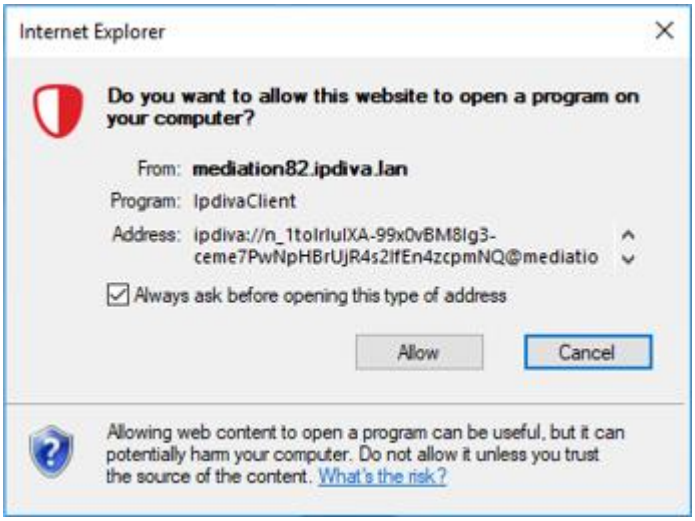
1- Identifiant utilisé pour se connecter au portail Systancia Gate
2- Informations concernant la dernière connexion effectuée avec ce compte utilisateur
3- Accès aux barres de filtres / recherche rapide
4- Catégorie(s) auxquelles appartiennent les différentes applications
5- Ressource(s) dont vous êtes autorisés à utiliser
6- Menu permettant d'accéder aux différents outils mis à disposition (.exe/ documentation) ainsi que les boutons de rafraichissement / à propos / déconnexion

4.2.2 Lancement d'une ressource

Le lancement d'une ressource Gate est assez simple, il suffit de cliquer sur l'intitulé de cette dernière pour qu'elle se lance.

Si la ressource sélectionnée est une ressource non-Web (ressource non utilisable au travers d'un navigateur web), alors celle-ci déclenchera l'utilisation du Client Gate pour l'activation de tous les services requis pour l'accès.

Une fois la ressource sélectionnée, un pop-up s'affiche vous demandant si vous souhaitez ouvrir un programme (IPdivaClient) sur votre ordinateur, cliquez sur « **Autoriser** ».

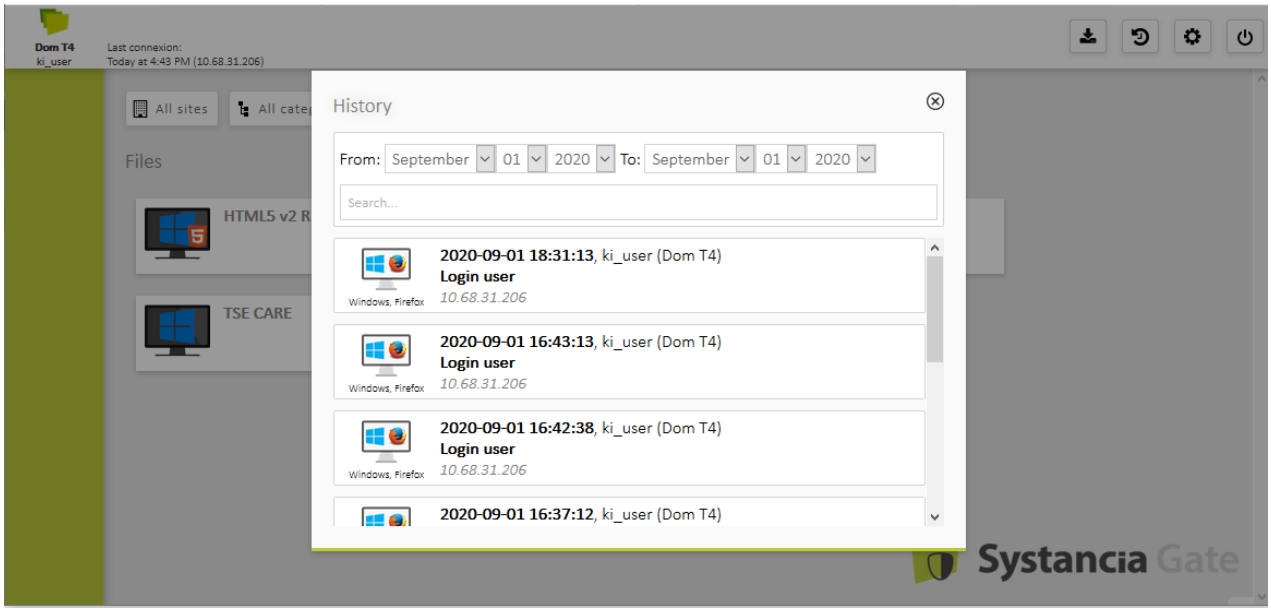


Un bandeau d'information indiquant l'état d'exécution (en cours de connexion / connecté…) apparait en bas à droite du bureau.

4.2.3 Historique

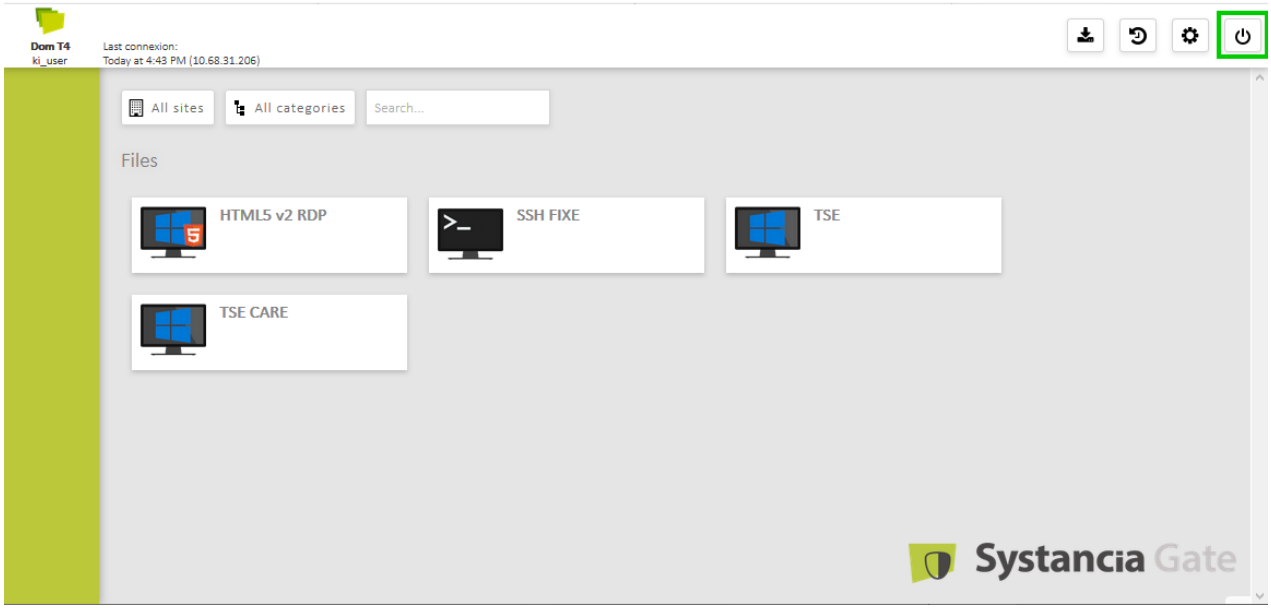
Le bouton historique permet d'accéder à une page récapitulant les dernières connexions avec les éléments suivant :

- Le nom d'utilisateur
- La date / heure de connexion de l'utilisateur
- L'adresse internet (IP) depuis laquelle il s'est connecté
- Le navigateur utilisé
- Le système d'exploitation utilisé



4.2.4 Déconnexion

La déconnexion est un processus important car elle évite l'utilisation frauduleuse de vos droits par un utilisateur malveillant à partir de votre terminal d'accès. Pour se déconnecter il suffit de cliquer sur le bouton de déconnexion :



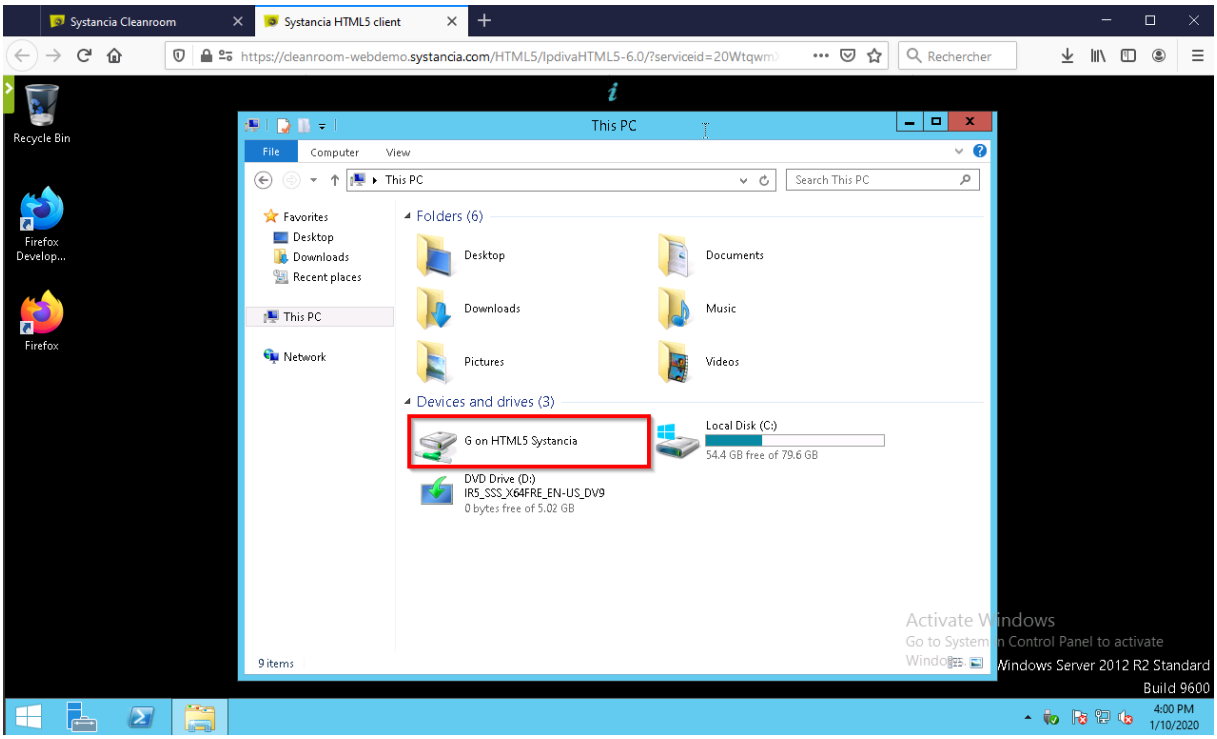
5. Mode HTML5 : Transfert de fichiers et Impression

Les ressources RDP, SSH et VNC peuvent être proposés en mode HTML5. Ce mode permet un affichage directement dans le navigateur sans avoir besoin d'installer de client sur le poste. Cette configuration est activée par l'administrateur lors de la création de la ressource.

5.1 Ressources RDP

- Transfert de fichier

Ce mode permet de transférer des fichiers à travers un partage de fichier temporaire appelé « G on HTML5 Systancia » (le nom peut varier en fonction de la configuration).



- Ressource vers Poste local :

Déposer un fichier dans le sous répertoire « Download » de ce partage temporaire déclenche automatiquement le téléchargement du fichier par le navigateur web.

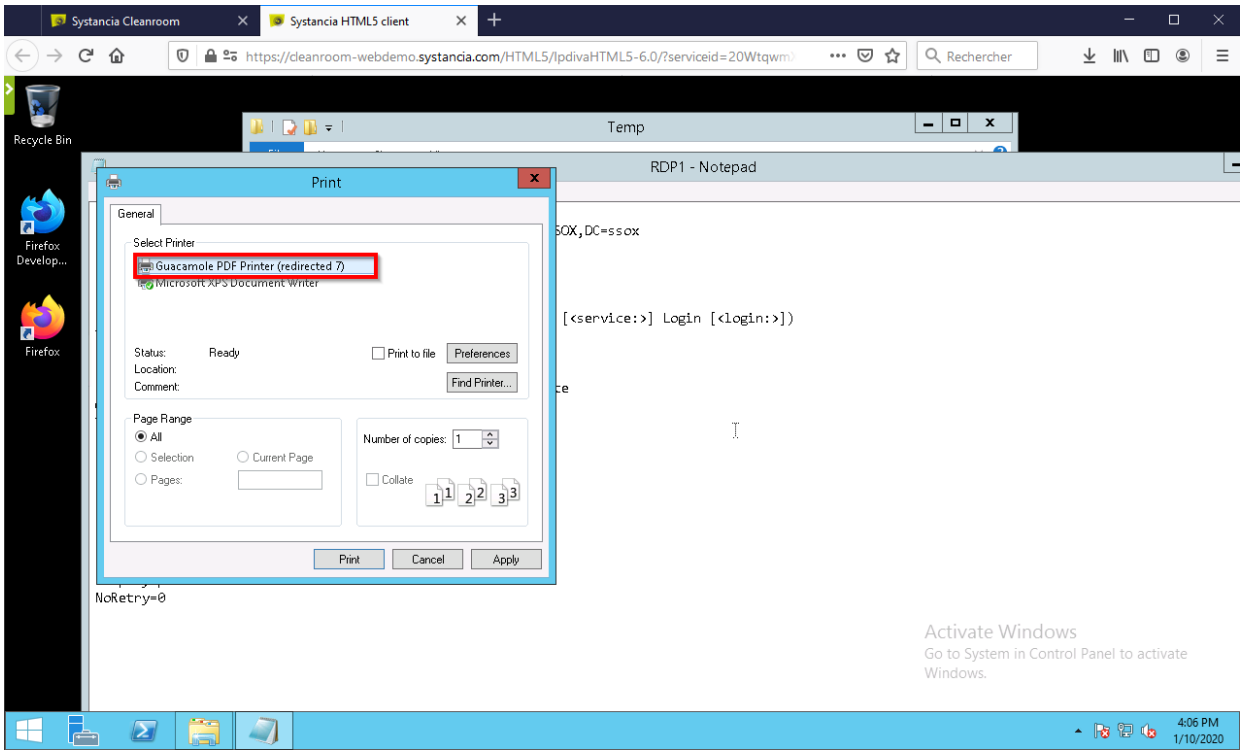
- Poste local vers Ressource :

Glisser-déposer un fichier sur le navigateur déclenche automatiquement l'upload du fichier.

Tous les fichiers présents dans ce répertoire sont supprimés automatiquement à la fin de la session.

- Impression

Il est aussi possible d'imprimer sur une imprimante locale en sélectionnant l'imprimante HTML5. Le nom peut varier en fonction de la configuration mise en place.



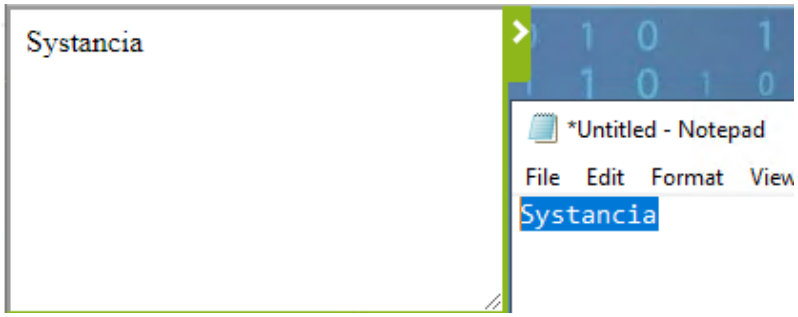
L'impression déclenche la génération d'un fichier PDF, qui est téléchargé par le navigateur et qui peut ensuite être imprimé sur une imprimante locale.

- Copier-coller

Il est possible de copier/coller du texte entre la ressource et le poste local.

Du poste utilisateur vers la ressource cela fonctionne naturellement via les raccourcis clavier ou les menus contextuels.

La copie de texte de la ressource vers le poste local déclenche l'ouverture d'une fenêtre dans le navigateur affichant le contenu du presse papier distant :



Il est ensuite nécessaire de copier à nouveau ce texte pour le récupérer dans le presse-papier local.

5.2 Ressources SSH

- Transfert de fichier

Lors de la connexion sur une ressource SSH, une variable d'environnement "SFTPSHARE" est automatiquement créée dans la session SSH.

  - Poste local vers Ressource

Pour transférer des fichiers, il suffit de glisser le ou les fichiers dans l'onglet de la ressource HTML5 SSH du navigateur client.

Une barre de chargement apparaît, et une fois l'envoi terminé, le fichier est disponible dans le répertoire $SFTPSHARE.

  - Ressource vers Poste local

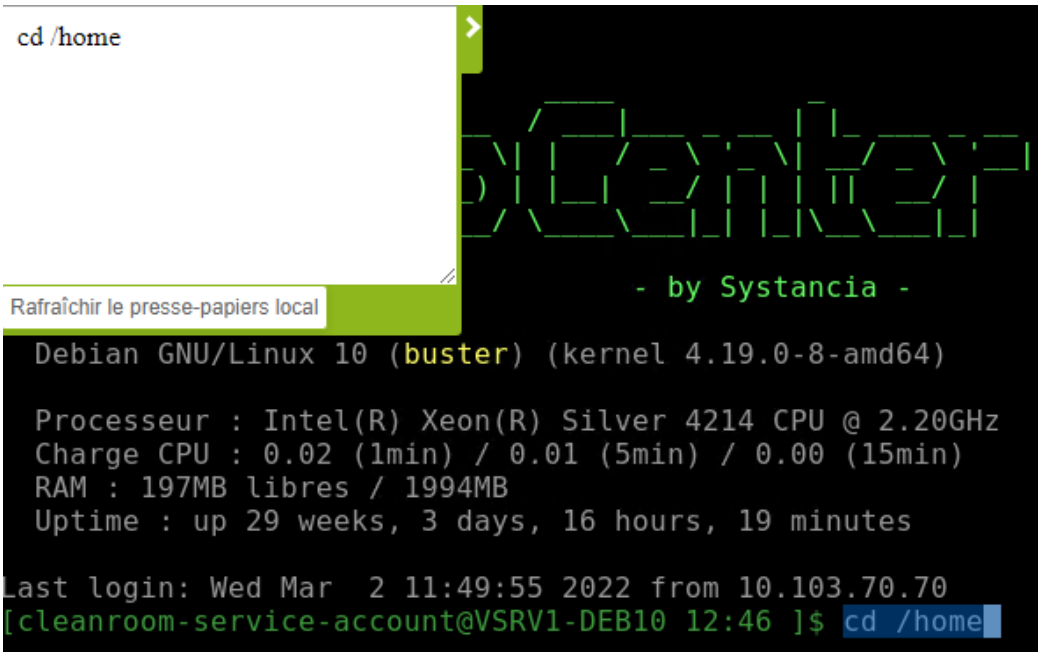
Pour télécharger un fichier depuis le serveur SSH, il suffit de copier ou déplacer un fichier vers le répertoire de partage $SFTPSHARE/Download.

Une fois la copie terminée, le navigateur propose le téléchargement du fichier.

- Copier-coller

Il est possible de copier/coller du texte entre la ressource et le poste local.

La copie de texte du serveur vers le poste local déclenche l'ouverture d'une fenêtre dans le navigateur affichant le contenu du presse papier distant :



Il est ensuite nécessaire de copier à nouveau ce texte pour le récupérer dans le presse-papier local.

Cette fenêtre sert aussi pour transférer le presse-papier local vers le presse-papier distant.

6. Incidents de fonctionnement

Différentes erreurs ou incidents de fonctionnement peuvent interférer avec le comportement de la solution Systancia Gate.

Certains de ces incidents sont liés à l'environnement d'accès IP/Internet utilisé (Réseau d'accès Internet encombré, routeur Internet éteint ou débranché, proxy d'accès Internet non configuré…). Nous vous recommandons de valider cet accès avant tout autre intervention sur la solution Systancia Gate.

D'autres incidents sont dus au fonctionnement général de la solution ou à des effets connexes interférant avec le fonctionnement correct de la solution. Ci-dessous quelques interprétations de ces incidents.

- **Constat** – Le portail affiche « Aucune passerelle connectée ».
  - Aucune passerelle d'interface avec les serveurs support des ressources n'est connectée dans ce site. Il peut s'agir d'une coupure d'accès Internet du côté du site hébergeant les ressources ou d'une intervention sur les règles de routage interne à ce site central.
- **Constat** – Le portail affiche « Aucun site ». Il en résulte qu'aucune ressource ne s'affiche à la connexion de l'utilisateur.
  - Aucun site n'a été défini par l'administrateur,
  - Aucune ressource n'a été définie par l'administrateur,
  - Aucun profil d'accès n'a été défini par l'administrateur,
  - Les profils utilisateurs définis par l'administrateur ne correspondent pas avec votre profil. Votre groupe, l'heure, la date, l'IP ou l'ordinateur de connexion n'est pas valide.

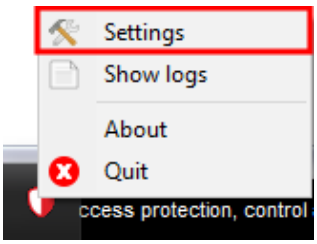
6.1 Unable to connect to remote host

Ce message d'erreur apparaît dans les logs du client Gate. Cela signifie que le poste client n'arrive pas à se connecter à la plateforme Systancia Gate.

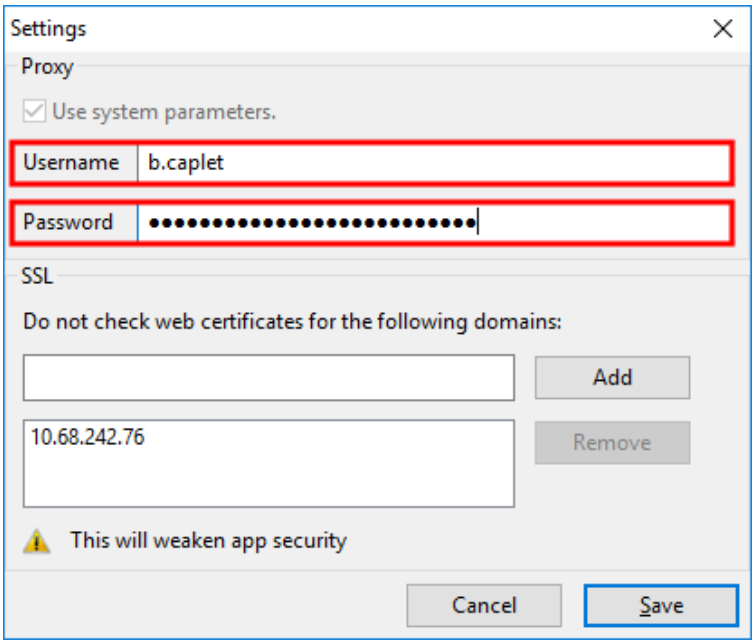
Dans la plupart des cas, ce message d'erreur est lié à l'utilisation d'un serveur proxy au sein de l'infrastructure.

Le client Gate récupère automatiquement les paramètres proxy d'Internet Explorer. Donc si vous avez ce message c'est que la configuration de ces paramètres est probablement incorrecte.

Si vous utilisez un proxy authentifiant : il faut configurer les identifiants dans le client Gate. Pour se faire, faites un clic droit sur le client Gate dans la barre de notification et cliquez sur « Configuration » :



Dans la configuration, vous pouvez entrer les identifiants pour l'authentification au serveur proxy :



Les autres causes sont généralement les suivantes :

- Un élément réseau ou pare-feu de l'infrastructure bloque la communication.
- L'antivirus sur le poste bloque la communication.
- La plateforme Gate n'est pas accessible.

SYSTANCIA

Actipolis 3, Bât C11

3, rue Paul Henri Spaak

68 390 SAUSHEIM

France

Téléphone : 03 89 33 58 20

Fax : 03 89 33 58 21

site web : https://www.systancia.com