Systancia

the human face of the workplace

SYSTANCIA GATE
Release Note

#Cybersecurity #Virtualization #AI

www.**systancia**.com

Ref. :	FR_Systancia-Gate-8.8_RN_rev.1.00
Version :	1.00
Produit :	Systancia Gate
Date :	2023-09-20

Objet :

Le document présente toutes les modifications techniques et fonctionnalités de la version 8.8 de Systancia Gate.

TABLE DES MATIERES

1. Principales nouveautés Systancia Gate 8.8

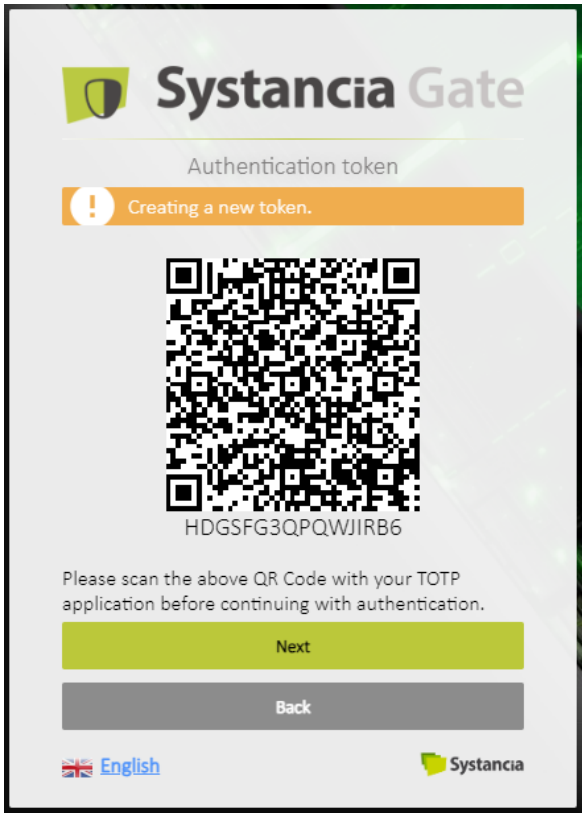
Cette nouvelle version apporte plusieurs corrections ainsi que quelques nouvelles fonctionnalités dont :

1.1 Support de Debian 11

Systancia Gate 8.8 ne supporte plus Debian 10 mais Debian 11.

1.2 Enrôlement des TOTP à l'aide de QRcode

Il n'est plus nécessaire de devoir paramétrer les smartphones des utilisateurs afin de leur ajouter la clef TOTP qui était soit stockée dans un attribut utilisateur ou soit stockée dans le produit mais envoyée par mail. Maintenant un QRcode à scanner avec l'application de TOTP est affiché lors de la première connexion de l'utilisateur :



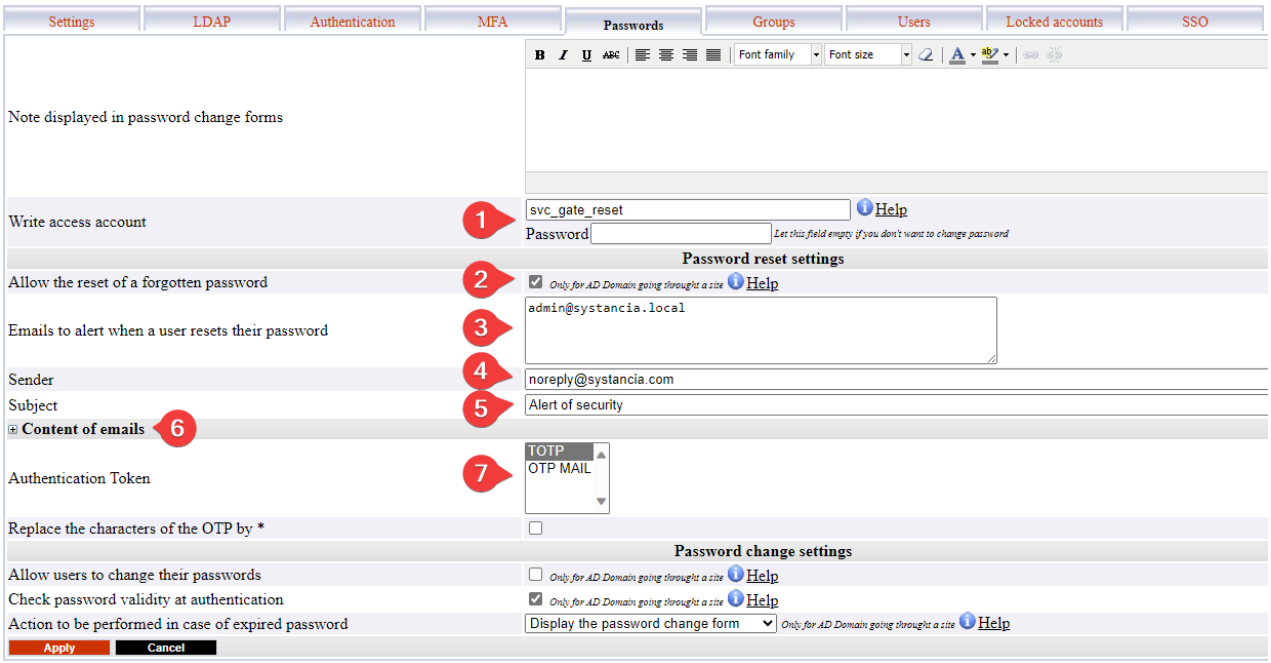
L'utilisateur devra ensuite valider son code afin que le produit ne lui affiche plus de QRcode.

Cette fonctionnalité n'est disponible uniquement que pour les clefs TOTP stockées par le produit, elle est donc incompatible avec l'option de récupération de la clef dans un attribut LDAP.

1.3 Self-Service pour la réinitialisation de mot de passe

Les utilisateurs peuvent maintenant être autonomes dans la réinitialisation de leur mot de passe en cas d'oubli. Pour ce faire, le produit demandera une preuve que la requête soit réalisée par la personne souhaitée à l'aide d'un jeton OTP.

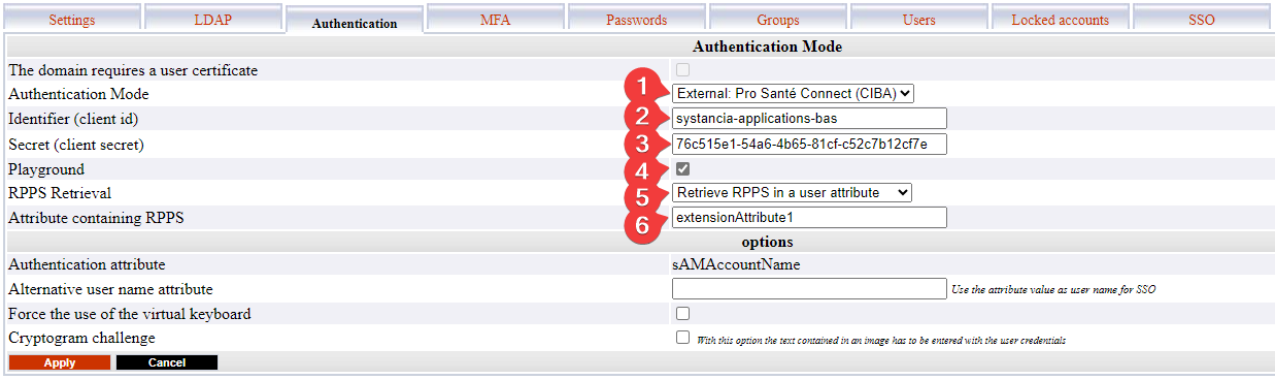
La configuration de cette fonctionnalité est réalisée dans le nouvel onglet « Mot de passe » des domaines :



1. Configuration du compte de service pour le changement des mots de passe ainsi que leur réinitialisation (si non défini utilisation du compte de service de lecture)
2. Activation de la fonction de réinitialisation de mot de passe
3. Adresses mail administrateurs à alerter lors de l'utilisation de la fonctionnalité, ces adresses recevront des copies des alertes envoyées aux utilisateurs (le mail des utilisateurs étant récupéré par l'attribut mail)
4. Adresse mail de l'expéditeur
5. Objet du mail d'alerte
6. Paramétrage des templates pour la tentative de réinitialisation ainsi que celui informant du succès de la réinitialisation
7. Choix du jeton d'authentification, un jeton étant obligatoire pour activer la fonctionnalité

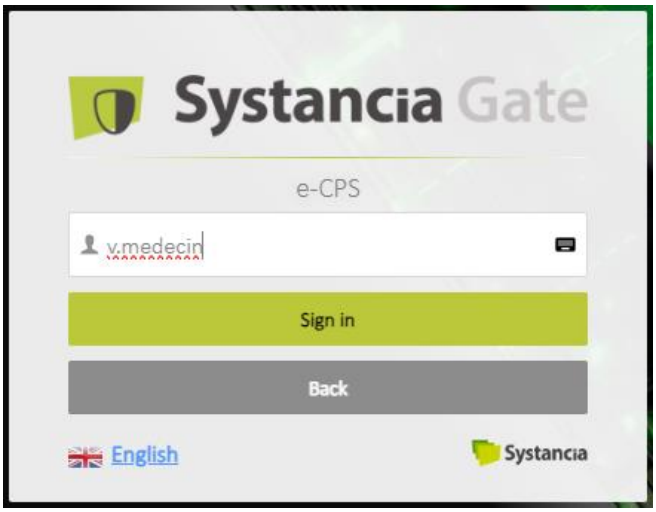
1.4 Support de l'authentification avec l'e-CPS de Pro Santé Connect

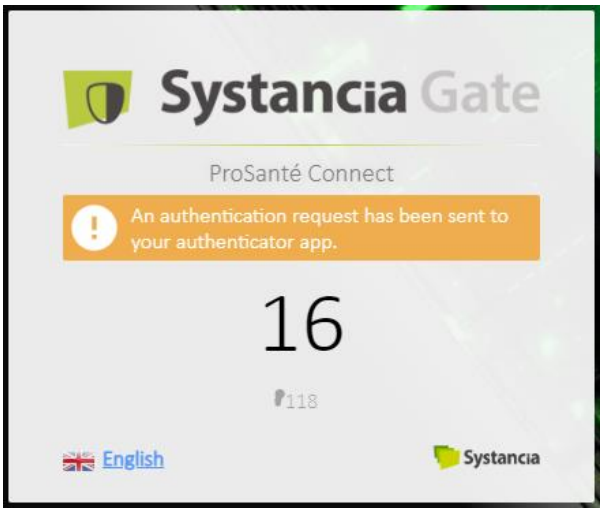
Systancia Gate 8.8 supporte la e-CPS de Pro Santé Connect pour l'authentification des utilisateurs, sa configuration se réalisant dans le nouvel onglet « Authentification » des domaines :



1. Configuration de l'authentification avec l'e-CPS en sélectionnant « Externe : Pro Santé Connect (CIBA) »
2. Votre identifiant client sur Pro Santé Connect
3. Votre secret
4. Si c'est une configuration pour un environnement bac à sable ou de production
5. Comment est récupéré le RPPS (soit par l'attribut d'authentification ou soit dans un attribut de l'utilisateur)
6. Dans le cas où le RPPS est récupéré dans un attribut utilisateur ce champ permet de préciser lequel il s'agit

Dans le cas de la configuration précédente, l'utilisateur s'authentifie avec son « sAMAccountName » et Systancia Gate ira rechercher son RPPS dans l'attribut « extensionAttribute1 ». Sur le portail cloud voici les deux étapes (saisie de l'attribut d'authentification puis réalisation de la connexion e-CPS) :

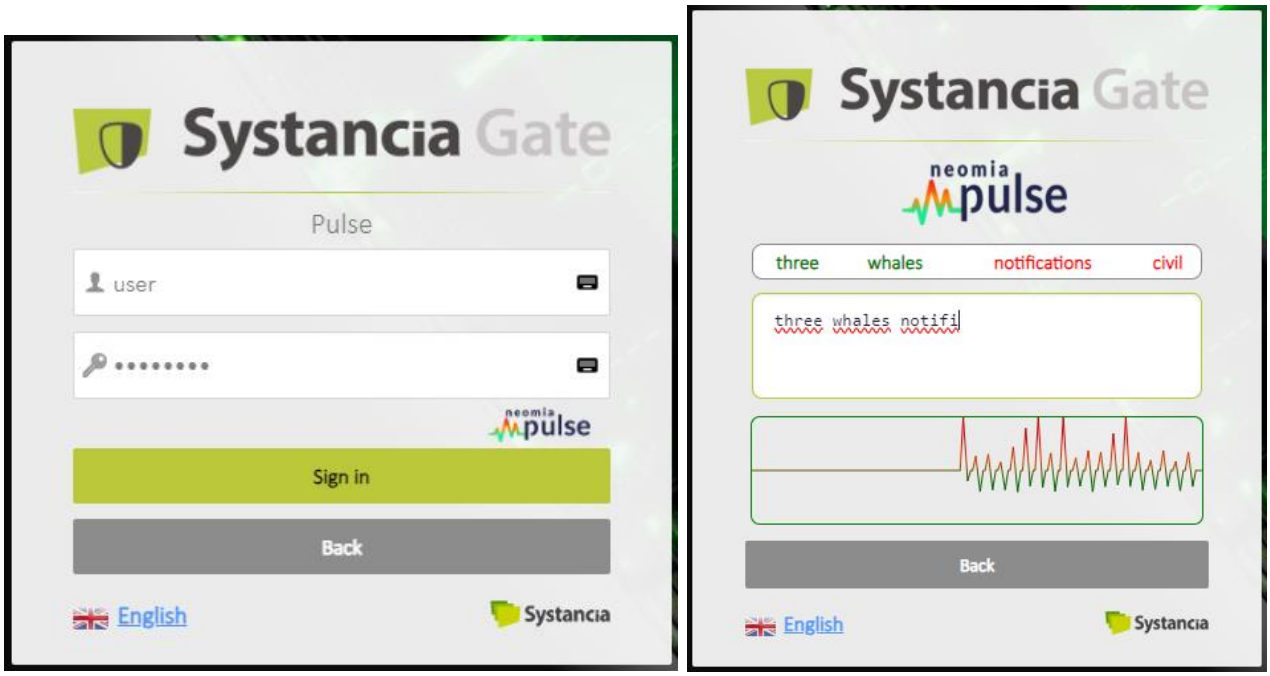




1.5 Disponibilité d'une analyse comportementale en MFA avec Neomia Pulse

Systancia Gate intègre un connecteur à Neomia Pulse qui est une intelligence artificielle d'analyse comportementale développée par Neomia, une filiale de Systancia. Neomia Pulse va déterminer une empreinte unique de la façon qu'ont les utilisateurs de taper les touches du clavier.

Cette analyse est utilisée dans Systancia Gate afin de ne pas avoir à saisir un MFA comme un OTP ou un TOTP. Cependant, si l'utilisateur n'est pas jugé de confiance il devra valider être l'utilisateur légitime en complétant un MFA.



Ci-dessus l'utilisateur s'authentifie de manière conventionnelle puis un nouveau panneau apparaît demandant de saisir quatre mots aléatoires ; c'est cette saisie qui servira à calculer l'empreinte de l'utilisateur tentant de se connecter. Si l'utilisateur est reconnu comme légitime il sera directement redirigé sur son portail avec ses ressources sinon un OTP lui sera demandé.

Pour plus d'informations sur le produit Neomia Pulse :

https://neomia.ai/la-biometrie-comportementale-en-70s/

1.6 Disponibilité de la Passerelle Systancia Gate au format Docker

Systancia Gate 8.8 introduit une nouvelle méthode de déploiement de ses Passerelles et Passerelles HTML5 : le déploiement via Docker.

Docker permet de ne plus être lié au socle OS et apporte donc la possibilité de déployer une Passerelle ou Passerelle HTML5 sur n'importe quelle distribution Linux.

Il est à noter que les Passerelles au format Docker possèdent toutefois deux fonctionnalités en moins par rapport à leurs homologues fonctionnant sous Debian :

- Le redémarrage journalier des services n'est plus disponible
- Les ressources VPN ne peuvent pas être exploitées avec les Passerelles Docker

2. Mises à jour / évolutions intégrées

Ci-dessous le récapitulatif des mises à jours/évolutions intégrées à la nouvelle version de Systancia Gate :

2.1 Sécurité

IPD inclus : 43855, 42453, 37020, 40501, 40543, 40735, 40546, 40732, 43173, 45022, 45110

- Mise à jour en version 2.29.4 de moment.js
- Prise en compte dans le journal Systancia Gate, pour le portail utilisateur, de l'adresse IP de l'utilisateur basé sur le header X-Forwarded-For
- Contrôle périodique de la règle MD5
- Affichage d'un avertissement sur l'interface system si Apache est paramétré pour autoriser une version antérieure à TLS 1.2
- La création de nouvelles organisations ne créera plus les comptes locaux « ipdivadmin » et « ipdivauser »
- Adaptation de l'affichage des profils d'accès en relation avec la configuration par défaut de modsecurity
- Support des authentifications multi-facteurs sur le domaine local, ainsi que pour la connexion des administrateurs
- Possibilité de restreindre certaines organisations à certains hôtes virtuels de type Web VPN
- Ajout de nouvelles entrées dans le journal pour tracer la réussite ou non du MFA pour une authentification utilisateur
- Les restrictions du nombre de tentative d'authentification ne tiennent plus compte de la casse pour les domaines LDAP
- Ajout d'une nouvelle option pour définir le nombre de tentative de connexion sur le formulaire d'authentification en cascade

2.2 Client Systancia Gate

IPD inclus : 44035, 42706, 42507, 36223, 31852, 42110, 40164, 39698, 41986

- Modification de la récupération de la configuration proxy : vérifie en premier la configuration présente dans HKEY_CURRENT_USER avant HKEY_LOCAL_MACHINE
- La configuration proxy du système n'est plus ignorée si le proxy est défini sur 127.0.0.1 ou 127.0.0.2
- Le client Systancia Gate pour MacOS est signé et reconnu par Apple
- Correction de l'affichage de deux icônes dans la systray pour Ubuntu 21.10
- Ajout de logs complémentaires dans le cas de l'échec de validation de la règle Windows Security Center
- Fiabilisation du client Systancia Gate sur Windows lorsque le poste possède des paramètres régionaux non supportés

2.3 Composants Mediation

IPD inclus : 42459, 40140, 45692, 44737, 44266

- Correction des défauts de connexion lorsque la connexion réalisée au routeur SSL est associée à un fichier dont le descripteur est supérieur à 1024
- Adresse de broadcast forcée sur celle de la VIP par le watchdog lorsque son masque de sous-réseau est /32
- La création des sauvegardes quotidienne n'est plus affectée par la configuration d'un proxy au niveau système sur le serveur Mediation
- Optimisation du poids des sauvegardes de configuration pour les clusters sur le Mediation Slave
- Fiabilisation de la connexion des Passerelles dans le cas où un recul de l'heure est paramétré sur le serveur Mediation

2.4 Portail utilisateur

IPD inclus : 43454, 42510, 40633, 39233, 40447, 33265, 42990, 44983, 44978

- Non affichage de l'installation du client Systancia Gate pour contrôler des règles si l'accès est réalisé via un appareil mobile (iPad, iPhone ou Android)
- Optimisation de la gestion des règles ne nécessitant pas le client pour afficher ou non les domaines disponibles
- Support de l'authentification par certificat avec des CN contenant des caractères accentués
- Support des caractères spéciaux dans le cadre d'une authentification par certificat avec fixation de l'identifiant par rapport au CN du certificat
- Ajout d'un message indiquant qu'aucune ressource n'est disponible pour l'utilisateur avec un bouton de rafraîchissement de la page

- Les différents formulaires d'authentification proposent le focus sur le premier champ
- Une option dans les paramétrages administrateurs permet de forcer la sélection d'un site lors de la connexion de l'utilisateur sur le portail utilisateur
- Le sélecteur du site a été amélioré pour proposer un champ de recherche des sites et un lancement après avoir appuyé sur la touche entrée

2.5 SAML

IPD inclus : 37745, 41283

- Révision du fonctionnement interne au produit sur le SAML, un besoin de reconfiguration du SAML sur la médiation est nécessaire
- Support d'un nombre de groupes renvoyés par l'IDP plus important

2.6 Mode VLAN

IPD inclus : 41957

- Correction de l'assignation des utilisateurs à leur VLAN respectif sur le portail cloud

2.7 Systancia Gate for Systancia Workplace

IPD inclus : 40246

- Ajout d'un exécutable nécessaire aux lancements sur le bureau des applications et bureaux Systancia Workplace

2.8 Console System

IPD inclus : 44772, 45529

- La modification du certificat plugin n'est plus réalisable si le mot de passe saisi est invalide
- L'utilisation d'un certificat placé sur un hôte virtuel affecte seulement la chaîne de certification liée à l'hôte virtuel et non plus à l'interface Web

2.9 Console d'administration

IPD inclus : 26556, 37629, 33426, 37749, 34345, 40690, 39663, 39270, 43890, 45789, 45508

- Remontée de la connexion des passerelles HTML5 ainsi que leur version et leur date d'expiration dans le sous-menu « Passerelles »
- Modification afin de récupérer l'IP publique, l'IP locale ainsi que la version du client Systancia Gate dans les informations détaillées des utilisateurs connectés
- Ajout d'une entrée dans le journal pour indiquer la présence de l'attribut utilisateur vide pour la récupération de la clef TOTP
- Révision légère de l'interface de consultation, création et modification des profils d'administration
- Ajout d'une nouvelle colonne dans la vue des sites pour y lister les passerelles HTML5 rattachées
- Ajout dans les utilitaires administrateurs d'un outil permettant de déchiffrer les fichiers d'export
- La suppression d'un OTP lié à des ressources ne provoquera plus le besoin de revalider la ressource sans OTP
- Modification du mail de notification généré afin de prendre en charge l'envoi à des destinataires multiples pour l'alerte d'ouverture de ressource
- L'importation d'utilisateurs locaux ne requiert plus la colonne « groups »
- Fiabilisation du mécanisme de duplication de ressource lorsque plusieurs services sont paramétrés

2.10 MFA

IPD inclus : 39463, 42945, 40696, 41611, 39749

- Le passage par un site pour l'accès à des API HTTPS n'est plus obligatoire
- L'importation de clef TOTP contrôle les informations données et remonte les clefs n'ayant pas pu être importées. Dans le cas où la clef est vide, la clef de l'utilisateur est supprimée pour qu'à la prochaine connexion de l'utilisateur elle soit regénérée
- Lors de la première connexion des utilisateurs ils pourront, si l'option est active, enrôler leur code TOTP à l'aide d'un QRcode
- Il n'est plus possible de récupérer la clef privée TOTP de l'utilisateur dans un de ses attributs pour les domaines locaux, cette fonction est réservée pour les domaines LDAP
- Gestion de ressources multi-services avec affectation d'un jeton OTP
- Gestion de l'affichage des caractères spéciaux sur les ressources (nom ou description)
- Ajout de nouvelles options pour l'OTP RADIUS : mode Push (envoi automatique d'un OTP invalide pour notifier l'authentificateur de l'utilisateur) ; timeout de connexion ; nombre d'essais et serveur secondaire

2.11 Configuration des domaines

IPD inclus : 43059, 42861, 42834, 42752, 42496, 42502, 42436, 42386, 36301, 26612, 37475

- Répartition en plusieurs onglets thématiques des options proposées dans l'onglet « Paramétrages »
- Modifications mineures d'affichage des utilisateurs locaux et du menu d'ajout d'utilisateurs locaux
- Autorisation de réinitialisation du mot de passe de l'utilisateur après l'utilisation d'un jeton
- Possibilité de définir un compte de service particulier pour les changements et réinitialisation de mot de passe utilisateur LDAP
- Ajout de l'option « SASL/DIGEST » aux domaines LDAP RADIUS
- Ajout d'une option pour les domaines SAML permettant d'indiquer l'hôte virtuel SAML afin que, si l'utilisateur se connecte avec l'hôte virtuel principal, il soit redirigé vers le bon hôte virtuel lors de l'authentification au domaine SAML
- L'import d'utilisateurs pour les domaines locaux nécessite un fichier CSV obligatoirement encodé en UTF-8
- Ajout de paramétrage d'une nouvelle demande de jeton OTP après la dernière connexion de l'utilisateur ou de la dernière saisie de l'OTP
- Ajout du support de l'e-CPS de Pro Santé Connect comme méthode d'authentification externe

2.12 Ressource RDP

IPD inclus : 45058

- Le lancement via une seule ressource de plusieurs services RDP est rétabli

2.13 Ressource VPN

IPD inclus : 36717, 43218, 37766, 35941, 39019, 21944, 36917

- Support de l'ouverture du VPN lorsque l'identifiant de l'utilisateur est supérieur à 34 caractères
- L'ouverture d'une ressource VPN bridge utilisant le DHCP local mentionne « VPN connecté » à l'utilisateur à la place de « IP obtenue : »
- L'option « lancer l'application » est maintenant supportée par l'agent GUI
- Modification du message affiché à l'utilisateur lorsque le VPN se reconnecte
- Correction de la prise en compte de la variable « %USERPROFILE% » dans la configuration de la ressource VPN
- Possibilité d'indiquer le masque réseau raccourci (exemple : /24) pour le réseau des utilisateurs

2.14 Ressources Web et reverse proxy

IPD inclus : 41010, 41255, 42547

- Réarrangement de l'interface de configuration du SSO
- Modification des cookies pour ne plus forcer l'ouverture d'une ressource Web ou reverse proxy si l'on ne s'est pas connecté à partir de leur virtual host
- Disponibilité du message d'erreur d'interdiction d'accès à une URL dans les autres langues que le français

2.15 Ressource Web

IPD inclus : 36359, 44113, 44425, 44391, 45052, 45111, 45348, 42946, 42955, 42922, 41562, 42406, 42116, 41943, 42086, 42085, 42084, 42115, 42130, 41751, 40574, 40568, 41622, 39812, 41030, 41049, 41434, 41514, 41521, 40332, 40259, 37795, 39634, 33852, 44207

- Ajout d'une option de redirection après SSO (compatible uniquement avec le SSO en préchargement de formulaire)
- Améliorations générales du fonctionnement des ressources Web pour son moteur de parsing et réécriture d'URL
- Amélioration du temps d'affichage des pages Web pour les versions antérieures à Firefox 105
- Amélioration du temps d'affichage des pages Web pour les navigateurs à base chromium
- Possibilité de paramétrer un hôte virtuel permettant l'ouverture de la ressource Web directement après l'authentification à Systancia Gate, de la même manière que le propose les ressources reverse proxy
- Possibilité d'ajouter des noms de domaines dans la configuration de la Passerelle à exclure de la réécriture d'URL, le format étant le suivant :

```
<gateway>
[…]
<webaccess>
      <rewrite-exclusions>
            <domain>localhost:64196</domain>
            <domain>www.systancia.local</domain>
      </rewrite-exclusions>
      […]
</webaccess>
[…]
</gateway>
```

2.16 Ressources SMB/NetBIOS

IPD inclus : 43986, 44055, 43424, 40840, 41249, 39857

- Support de DFS
- Amélioration de la gestion de dossiers contenant énormément de fichiers
- Correction de l'enregistrement de fichiers de taille inférieure au fichier d'origine

2.17 Ressource SMB

IPD inclus : 37373

- Evolution de l'aspect visuel de la ressource, cette dernière s'adaptant à la personnalisation du portail utilisateur (couleur dominante + logo)

2.18 Ressources HTML5

IPD inclus : 43761, 43706, 37639, 42520, 42048, 41347, 11464, 41256, 43821

- Autorisation de transfert de fichiers d'une taille supérieure à 2Go
- Optimisation de l'usage de la RAM lors d'un transfert de fichier
- Ajout d'un paramètre au niveau de la ressource pour autoriser ou non le transfert de fichiers HTML5
- Correction du SSO sur les ressources HTML5 lorsque l'authentification composite est activée au niveau des domaines
- L'utilisation exclusive de ressources HTML5 n'entraîne plus la déconnexion de l'utilisateur sur inactivé
- Amélioration de la gestion de la saisie avec auto-complétions des claviers des smartphones
- Précision du défaut de connexion de la ressource entre : l'erreur de connexion ; identifiant SSH incorrect ; serveur SSH non joignable et serveur VNC non joignable
- Correction du lancement des ressources HTML5 RDP lorsque le SSO demandé est activé
- Les ressources HTML5 RDP proposent par défaut le paramétrage de sécurité placé sur « any »

2.19 Ressource Citrix Storefront

IPD inclus : 42887

- Support du lancement de bureaux ou d'applications Citrix dans le navigateur

2.20 Ressource SSH

IPD inclus : 41020

- Sur macOS, prise en compte de l'utilisateur saisi sur le portail cloud pour l'ouverture de la session SSH

2.21 Ressource VMware Horizon View

IPD inclus : 40611, 40528, 40694, 40730

- Ressource « VMware View » renommée en « VMware Horizon View »
- Corrections sur le fonctionnement de la ressource

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 : http://www.SYSTANCIA.com