A more human resource.

INTERNATIONAL PRODUCTION CENTER

97-Préconisations Techniques Offres de services Web ADP

V4.1 ► Janvier 2017

Confidentiality: ADP

The information contained in this document is privileged and confidential, and remains the intellectual property of ADP. This document must be kept strictly confidential at all times. It must not be disclosed to any person other than on a business need to know basis.

Sommaire

Descriptif

Titre	97-Préconisations Techniques Offres de services Web ADP
Version	4.1 Mars 2017

Diffusion spécifique

Destinataire	Entité
CLIENTS DES OFFRES DE SERVICES WEB D'ADP	

Attention : Vous êtes destinataire de ce document. A réception, vous devez:

- Détruire tout exemplaire antérieur en votre possession.
- Informer vos collaborateurs de la mise à jour.

1. PRESENTATION

Ce document décrit les caractéristiques techniques des offres de service Web d'ADP ainsi que les préconisations à respecter sur les postes utilisateurs ou le réseau du client pour un fonctionnement optimal de l'application hébergée chez ADP GSI France.

Les sujets abordés sont : Le réseau, le poste utilisateur et le paramétrage du navigateur Web, la sécurité, la messagerie et le requêteur Web Intelligent.

Pour toute question sur ce document vous pouvez ouvrir un ticket à la Help Line d'ADP au **0825 333 223 (N° Indigo 0,15 €/Min) ou** helpline.clients@fr.adp.com

2. LA CONNEXION AU PORTAIL D'ADP

2.1. Introduction

Les applications sont disponibles sur l'Internet public et sont hébergées dans le centre de production d'ADP.

INTERNET
Connexion sécurisée : HTTPS

L'accès aux applications est disponible depuis un point d'accès Internet (site de la société du client, domicile, hôtel, etc.).

Depuis le site du client, celui-ci est le seul responsable de son accès Internet (choix du fournisseur d'accès, dimensionnement de la liaison, sécurité de la liaison).

L'accès aux services ADP via Internet est ouvert à tous les utilisateurs disposant d'une authentification chez ADP gérée par le client.

2.2. Schéma de connexion par INTERNET

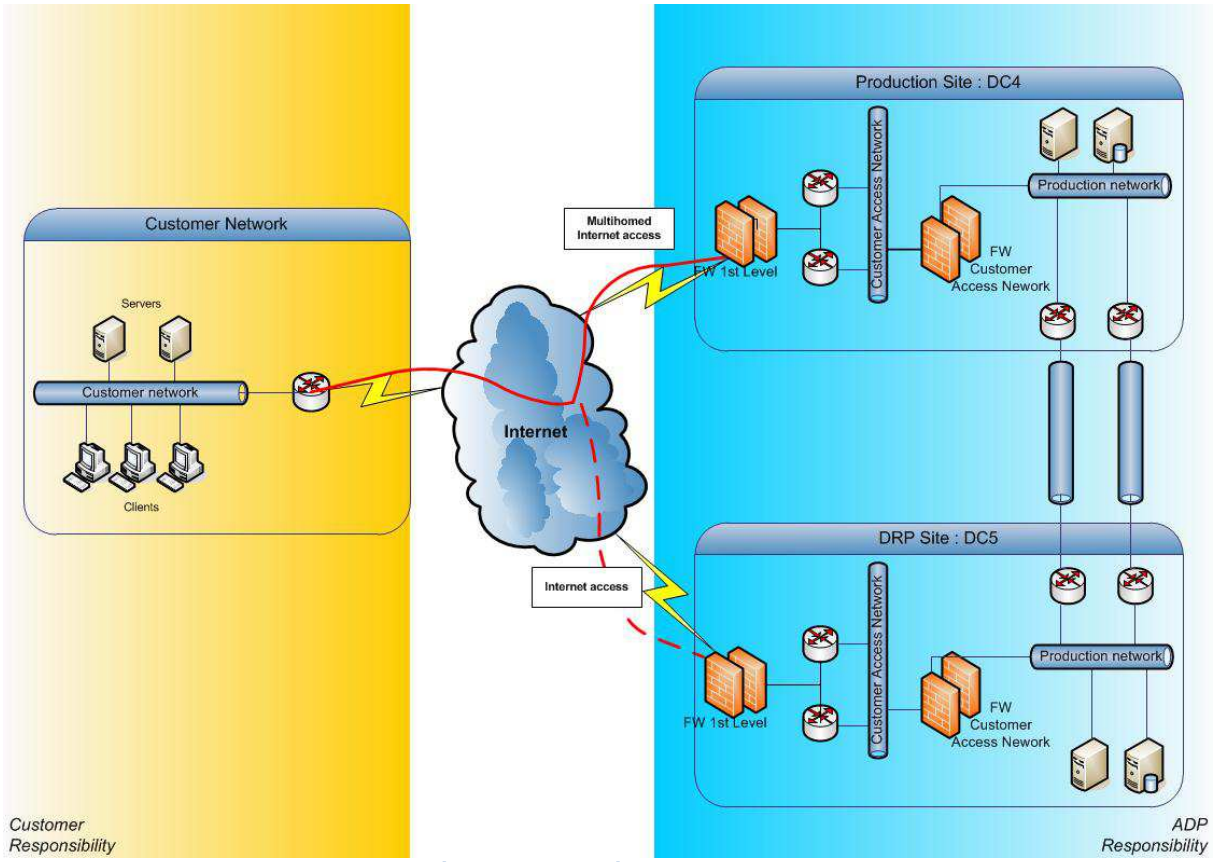


Figure 1 Connexion par Internet

Choix du fournisseur d'accès

Le client est entièrement responsable du choix de son fournisseur d'accès Internet.

Débit de la liaison
Le client doit s'assurer auprès de son fournisseur de la qualité de sa bande passante et du débit garanti (voir le tableau du calcul de la bande passante au paragraphe volumétrie ci-après).
Une analyse régulière de la charge est conseillée.

Sécurité de la liaison
Le client doit s'assurer de la sécurité de sa liaison :
- durée du rétablissement en cas de coupure ou de panne matériel,
- liaison de secours (Backup de ligne).

2.3. URLs des offres de services Web ADP

ADP utilise le protocole HTTPS (port 443) standard.

Liste des URLs des Applications ADP :

Portail des Applications : http(s)://hr-services.fr.adp.com
Application Z@DIG
http(s)://www.lsprh.adp.com
Gestion des droits
http(s)://www.duma.adp.com
Gestion des Flux Financiers (Virements et Paiements)
http(s)://www.gff.adp.com
Echanges de Fichiers (Gateway)
http(s)://www.zft.adp.com
Déclarations
http(s)://www.dadsu.adp.com
http(s)://www.ducs.adp.com
Déclaration Sociale Nominative
http(s)://hr-services.fr.adp.com/dsn
Assistance et Suivi Client
http(s)://www.symphony.adp.com
Attestations Pôle Emploi
http(s)://www.ape.adp.com
Attestations IJSS
http(s)://www.ijedi.adp.com
Expérience utilisateur
http(s)://mon.adp.com

Ces URLs sont fixes et ne peuvent être modifiées :
Les offres ADP ne peuvent pas fonctionner en dehors de ces adresses.
La résolution de ces URL doit impérativement être effectuée par les DNS publics d'Internet et en aucun cas par un quelconque système de résolution de nom propre à votre réseau d'entreprise, qu'il soit local ou étendu.

2.4. Volumétrie

Calcul de la bande passante
La bande passante consommée par un client est estimée à partir du nombre d'utilisateurs simultanés et de données provenant des tests de charge effectués sur des plateformes clients.

Les valeurs de bandes passantes mentionnées ci-dessous font référence à des débits requis qui doivent être dédiés à l'application.

La bande passante **minimum** par site doit être de **128 Kbit/s en download** et **64Kbit/s en upload** même si le nombre d'utilisateurs est très réduit.

La bande passante requise par **utilisateur simultané** est de :
- **25 kb/s** en débit descendant (download),
- **10 kb/s** en débit remontant (upload).

Cette évaluation de bande passante doit être respectée aussi bien au niveau de la liaison globale avec ADP concernant l'effectif total (si cette liaison existe) que de chaque liaison inter-sites en fonction des effectifs respectifs des différents sites (si les données à destination d'ADP transitent par ces liens).

Il apparaît que dans le cadre d'un mode d'utilisation standard, le nombre d'utilisateurs simultanés en pic représente environ **2.5%** du nombre total de collaborateurs traités par le SI.

Le tableau ci-dessous répertorie une évaluation du besoin global en bande passante correspondant à un effectif donné.

Site	Exemple 1	Exemple 2	Exemple 3	Exemple 4
Nb de collaborateurs	250	500	1000	1600
Nb de collaborateurs utilisant simultanément le produit	7	13	25	40
Ligne correspondant au débit descendant nécessaire (en Kbit/s)	256	512	1024	2048
Ligne correspondant au débit montant nécessaire (en Kbit/s)	128	256	512	512

Figure 2 Evaluation du besoin global

3. PREREQUIS

3.1. Prérequis du poste utilisateur

La résolution minimum de l'écran est de **1280x800**
Préconisation : utiliser un format **16/9ème**

Pour la fonctionnalité **« Contrat »** de l'application **Z@DIG**, les polices supportées dans les maquettes Word sont : Arial et Times New Roman.

3.1.a. OS supportés sur le poste de travail

Microsoft Windows

Version minimum:	Windows 7 SP1
Version recommandée:	Windows 10
Version maximum:	Windows 10

3.1.b. Navigateurs supportés sur le poste de travail

Internet Explorer

Version recommandée :	Internet Explorer 11
Version maximum :	EDGE

Firefox
Version : ADP garantit la compatibilité sur les versions récentes.
URL de téléchargement : http://www.mozilla-europe.org/fr/

Chrome
Version : ADP garantit la compatibilité sur la version en cours.
URL de téléchargement : https://www.google.com/chrome

Particularités :

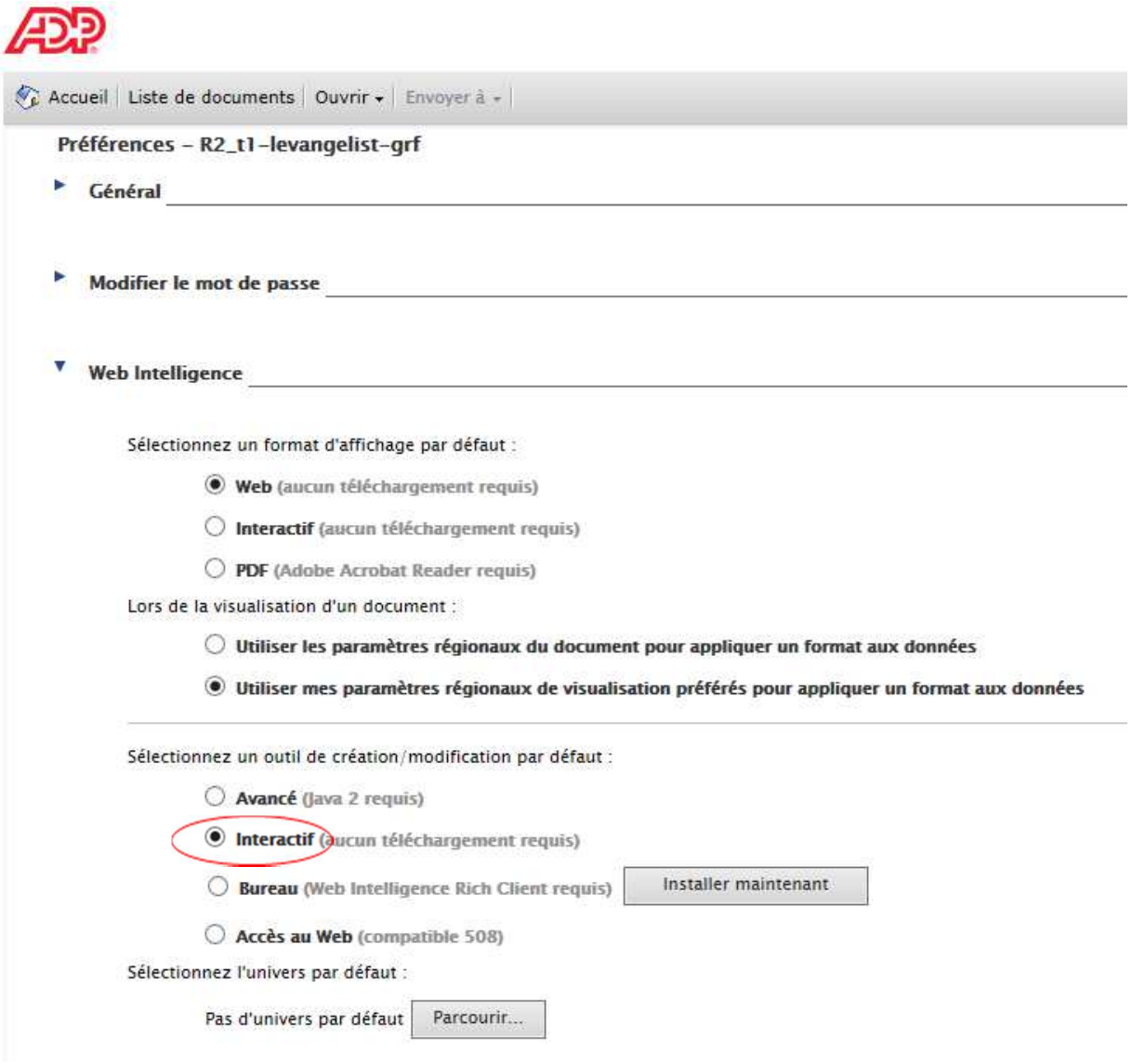
NPAPI (technologie requise pour les applets Java) n'est plus pris en charge par :

- Google Chrome depuis la version 45
- Firefox depuis la version 52 (Seules les versions de la branche **ESR** resteront compatibles avec les Applets Java jusqu'en 2018)
- EDGE

1. **Pour les contrats et virements nécessitant des applets de signature électronique Java ADP recommande :**
   Internet Explorer 11

2. **Pour les experts utilisant le requêteur Lsprh Web Intelligent Z@DIG (BO : Business Object), ADP recommande** :
   Internet Explorer 11
   Ou
   Sélectionner le mode Interactif de BO (pour lequel Java n'est pas utilisé).

(Onglet préférence/Web Intelligence/ Sélectionnez un outil de création/modification par défaut -> cocher **Interactif**
(Note : Le formatage conditionnel (alerteurs) et les sous-requêtes BO ne sont pas disponibles en mode Interactif)



3.1.c. Logiciels installés sur le poste de travail

Acrobat Reader
Version minimum: Acrobate Reader 8.x
Version maximum : versions supérieures
URL de téléchargement : http://www.adobe.com

Plug-in Java Runtime environnement pour Windows
Ce plug-in Java est nécessaire pour les postes qui utilisent le requêteur Web Intelligent Z@DIG (BO : Business Object).
avec **Internet explorer 11**
Sun 1.8.0_xx
URL de téléchargement : http://www.oracle.com/technetwork/java/index.html
http://www.oracle.com/technetwork/java/archive-139210.html

Ce Plug-in doit être capable :

- d'importer des certificats de type applet signé (via l'application de configuration du Plug-in ou en ligne de commande avec keytool),
- d'exécuter des applets signés.

Business Objects est mis en œuvre au travers d'une applet nécessitant l'installation d'un certificat signé.

- SAP AG
  Panneau de configuration Java => Onglet « Sécurité » => Cliquer sur « Gérer les certificats »

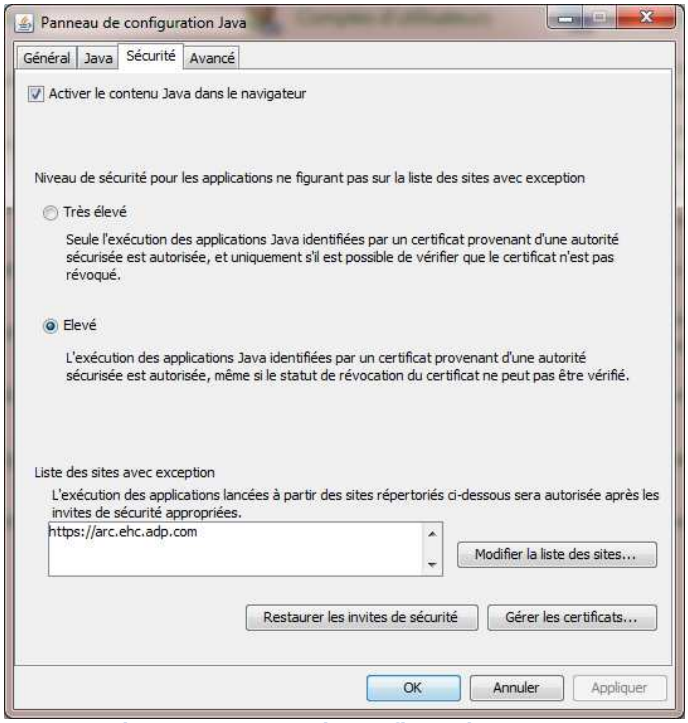


Figure 3 Panneau de configuration Java

Importer le certificat.

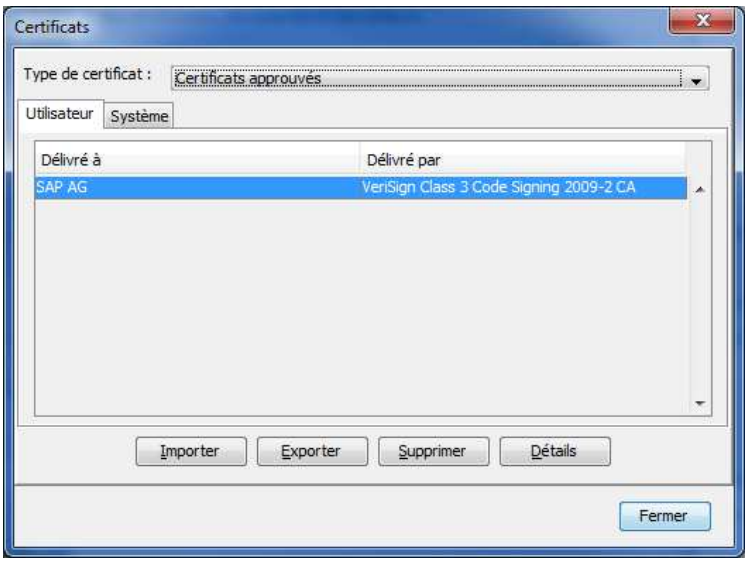


Figure 4 Certificats approuvés

3.1.d. Configuration du matériel

CPU	x86 1GHz minimum ou plus suivant le système d'exploitation
Mémoire	2 Go minimum ou plus suivant le système d'exploitation
Ecran	XGA (Couleur Moyenne ou Optimale) Résolution minimum 1280x800
Système d'exploitation	Windows 7 SP1 jusqu'à Windows 10

3.1.e. Paramétrage Internet Explorer

Le navigateur doit autoriser les pop-ups et les cookies.

« Outils », « Options Internet »
Onglet « Général »
Historique de Navigation « Paramètres »
Vérifier s'il existe une version plus récente des pages enregistrées → l'option **« Automatiquement »** doit toujours être cochée.
L'espace disque à utiliser doit être de **400Mo.**

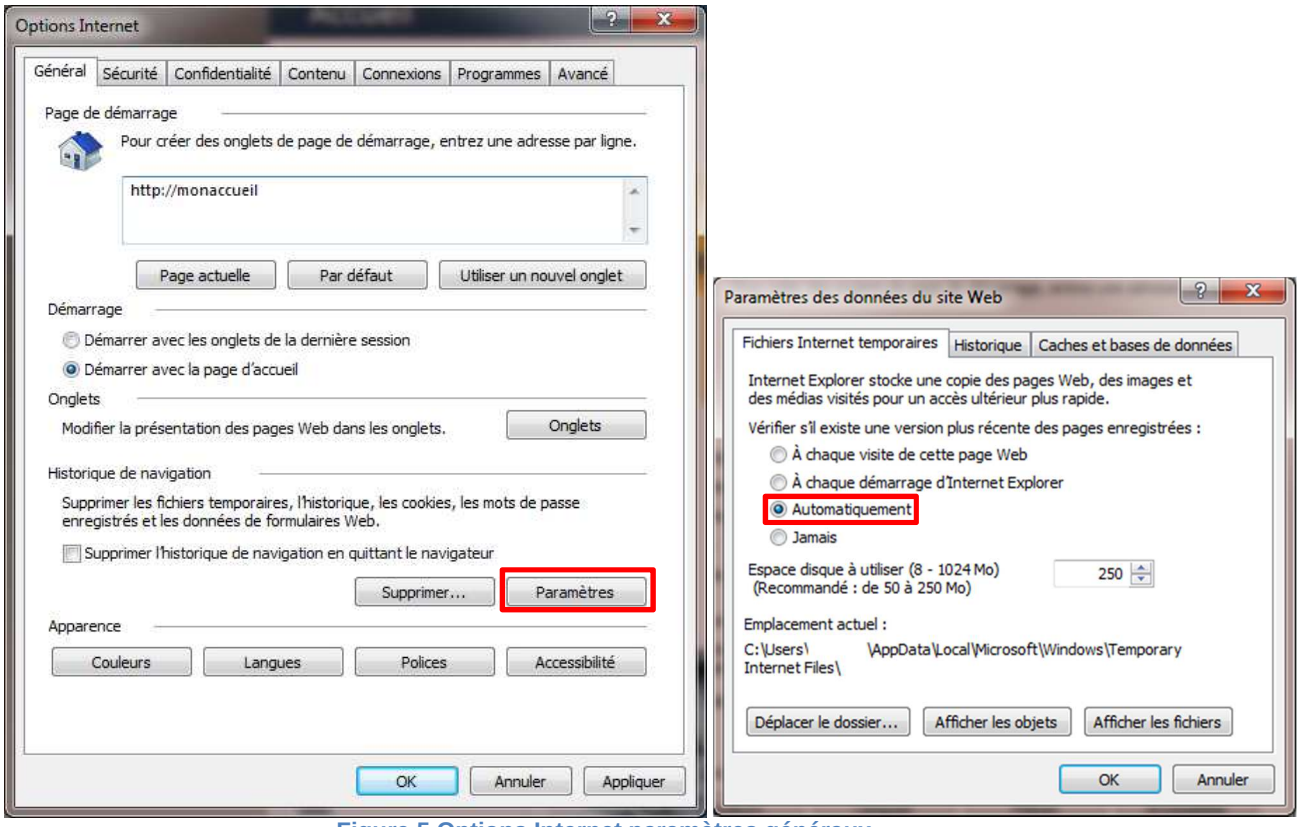


Figure 5 Options Internet paramètres généraux

Onglet « Sécurité »
Entrer dans les sites de confiance d'Internet Explorer, bouton **« Sites »** https://hr-services.fr.adp.com et https://www.zadig-hr.adp.com

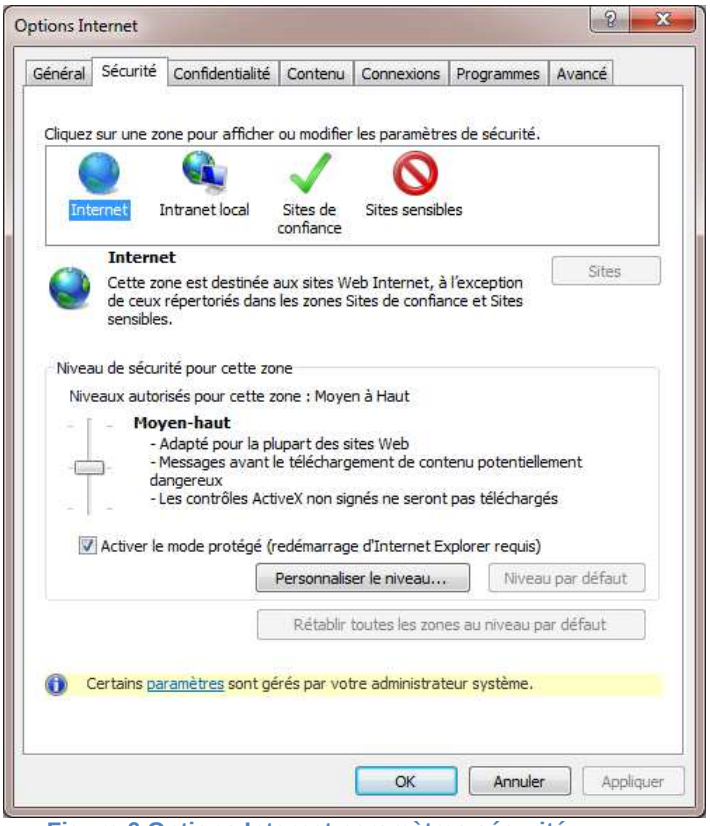


Figure 6 Options Internet paramètres sécurité

Cette action doit être effectuée avec le rôle administrateur système.

Onglet « Confidentialité »
Le navigateur doit accepter les cookies : la barre de niveau doit être positionnée à **« Moyenne »**

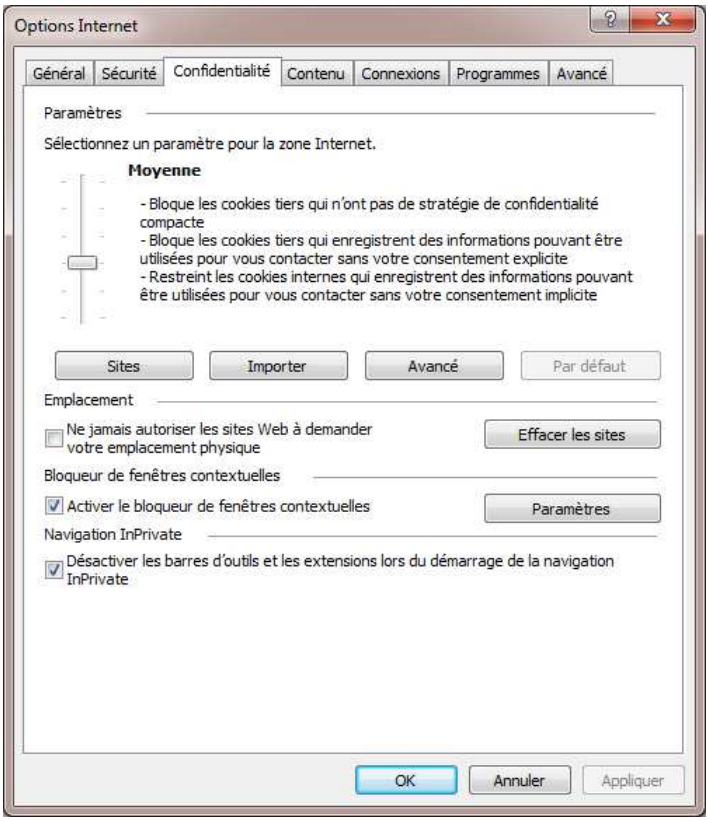


Figure 7 Options Internet paramètres confidentialité

Onglet « Avancé »
Chapitre « Impression en cours », la zone imprimer les images et les couleurs d'arrière-plan doit être activée
Chapitre « Paramètres HTTP 1.1 », la zone utiliser HTTP1.1 doit être activée
Chapitre « Paramètres HTTP 1.1 », la zone utiliser HTTP1.1 avec une connexion par proxy doit être activée
Chapitre « Sécurité », la zone « Vider le dossier Fichiers Internet temporaires lorsque le navigateur est fermé» doit toujours être désactivée.

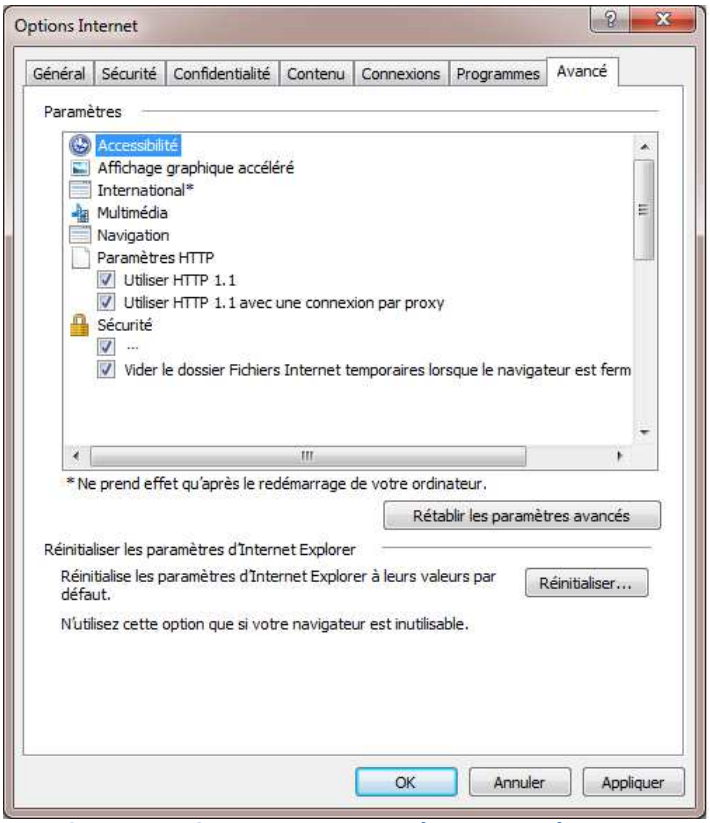


Figure 8 Options Internet paramètres avancé

« Outils », « Paramètre d'affichage de compatibilité »
Le site adp.com **ne doit pas** être ajouté dans les listes des paramètres d'affichage de compatibilité.

Nous vous recommandons d'effectuer régulièrement les mises à jour sécurité de votre système d'exploitation et navigateur Internet, notamment des certificats Windows.

3.2. Imprimantes

Les restrictions sur les imprimantes sont liées aux états qui peuvent être volumineux en retour du central pour impression sur le poste de travail.
- Bulletin de paie
- Attestation Assedic, …

ADP préconise une imprimante 15 pages par minutes minimum.

3.3. ADP Mobile Solutions

ADP Mobile Solutions est une application mobile en libre-service, accessible au salarié, qui permet de rester connecté aux informations de l'entreprise, à tout moment et de n'importe où.

Lorsque vous accéderez à l'application, vous ne verrez que les informations RH, issues des applications ADP, auxquelles votre société permet l'accès depuis votre mobile.

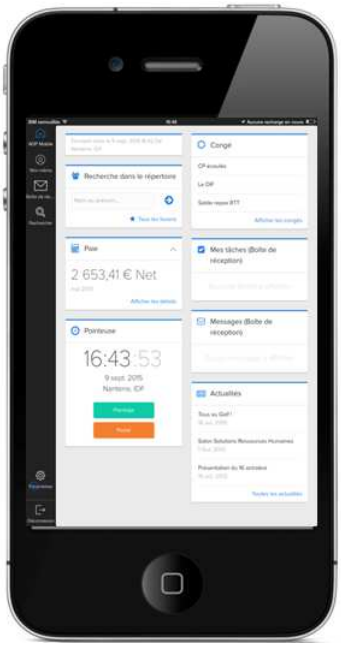


Figure 9 ADP Mobile solutions

Prérequis :

- Terminal mobile
  - ➢ iPhone® : 3G,3GS, 4, 4S, 5, 6 avec iOS 4.0 ou supérieur
  - ➢ iPod touch® 3ème ou 4ème génération avec iOS 4.0 ou supérieur
  - ➢ iPad® iOS 4.0 ou supérieur
  - ➢ Android™ 2.0 ou supérieur
  - ➢ BlackBerry® 4.6.1 ou supérieur
- Connexion à internet
- identifiant et mot de passe pour une application ADP

Téléchargement de l'Application :

Téléchargement gratuit de l'application *ADP Mobile Solutions* sur l'Apple Store ou Play Store pour les utilisateurs équipés d'i phone, i pad ou smartphone Android.

(***rechercher ADP Mobile Solutions***)

Connexion à l'application : https://mobile.adp.com pour les utilisateurs non équipés de smartphones.

Sécurité :

- Toutes les requêtes et transactions transitent par les serveurs sécurisés d'ADP.
- Tous les échanges sur le réseau entre l'appareil mobile et le serveur sont cryptés.
- Protection par identifiant et mot de passe (ou code PIN à choisir dans les Paramètres).
- Les sessions sont déconnectées après une période d'inactivité.
- Le compte est verrouillé en cas d'échec de connexions successives.
- Toutes les informations du salarié dans le cache du mobile sont cryptées.

4. LA SECURITE

4.1. Charte sur l'utilisation de l'Identification (Compte utilisateur)

L'identifiant est unique pour un même utilisateur.
La composition de l'identifiant ADP est la suivante :
<code prénom><code nom>-<code aléatoire>

Caractères	
1	Première lettre du prénom <code prénom>
2-10	Dix premières lettres du nom <code nom>

Si le prénom est composé (composé = présence du caractère '-')

Caractères	
1-2	Deux premières lettres du prénom <code prénom>
3-10	Neuf premières lettres du nom <code nom>

Caractère	
-	Le tiret

Caractères	
1-2	3 caractères alphanumériques aléatoires <code aléatoire>

4.2. Charte sur l'utilisation de l'Authentification (Mot de passe)

L'authentification engage la responsabilité de l'utilisateur

- L'authentification permet au contrôle d'accès logique de s'assurer que l'utilisateur identifié est bien celui qu'il prétend être.
- Tout utilisateur possède un authentifiant connu ou possédé de lui seul.

Le mot de passe

- Expire au bout de 120 jours, 10 jours d'alerte avant expiration pour changement à effectuer,
- Etre différent à 50% du précédent,
- Ne peut pas être réutilisé pendant au moins 4 générations,
- Ne peut pas être égal à l'identifiant, ne peut pas contenir l'un des attributs de l'utilisateur (si prénom=christophe, christophe8 sera refusé),
- N'apparaît jamais en clair à l'écran. Au bout de 6 tentatives successives infructueuses, le compte de l'utilisateur est désactivé.

Les mots de passe doivent respecter les règles de syntaxe suivantes

- Une longueur minimum de 8 caractères.
- La longueur maximale du mot de passe est de 16 caractères.
- Il comportera au moins un caractère numérique et au moins un caractère alphabétique.
- Majuscule, minuscule, ponctuation et caractère non alphanumérique accepté.
- Le mot de passe ne doit pas comporter plus de 3 caractères identiques à la suite : frdmmmmuik3 et chris4444 sont interdits.

Les administrateurs n'ont pas la possibilité de connaître les mots de passe des utilisateurs.

- Ils ont la possibilité d'initialiser un mot de passe pour un nouvel utilisateur et pour celui qui aurait perdu le sien,
- Le programme contrôlant l'accès forcera l'utilisateur à changer le mot de passe dès la première connexion.

Compte inutilisé

- Au bout de 360 jours de non utilisation le compte est bloqué. Seule une intervention de l'administrateur pourra le débloquer.

4.3. Déconnexion automatique de session (Time Out)

Une nouvelle authentification (Identifiant + Mot de Passe) est demandée après 30 minutes d'inactivité sur une application ADP.

4.4. Audit

Enregistrement des événements survenus

L'ensemble des événements sur le service d'identification/authentification est enregistré.

5. MESSAGERIE ELECTRONIQUE

5.1. Prérequis

Seule les messageries de type Internet sont compatibles (xxxx@domaine).
Chaque utilisateur doit posséder une adresse Email publique résolue sur Internet

Des courriels sont générés lors des évènements suivants :

- Attribution de l'identifiant de l'utilisateur,
- Modification du Mot de Passe,
- Tout autre processus prévu dans l'application et mis en œuvre pour le client.

5.2. Serveur SMTP ADP

Pour information, afin de vous permettre d'adapter vos éventuelles règles de filtrage, le FQDN du serveur smtp d'ADP relayant les mails du système est le suivant : **smtp.ehc.adp.com**

5.3. Comment ADP protège contre le phishing

Dans un souci d'aider les organisations à se défendre contre les attaques de phishing avancées et les communications électroniques frauduleuses cherchant à exploiter la marque de confiance ADP, ADP utilise DMARC (Domain-based Message Authentication, Reporting and Conformance) pour ses systèmes de messagerie.
DMARC est un standard public libre destiné à réduire l'usage des falsifications d'adresse d'expéditeur et de nom de domaine. DMARC confirme aux produits anti-phishing compatibles, utilisés par nos clients, qu'un message est envoyé légitimement par ADP ou par l'un de ses partenaires de confiance.

DMARC aide à déterminer si un email provient d'une source légitime en validant l'adresse et le domaine de l'expéditeur un peu comme un tampon valide l'adresse de retour d'un courrier postal. Alors qu'il est possible de créer une fausse adresse de retour, un peu comme une fausse adresse e-mail, un cachet de la poste ne peut pas être falsifié. DMARC met une «marque post » sur les e-mails provenant d'expéditeurs légitimes pour assurer qu'ils sont sûrs. Les organisations et les entreprises qui sont capables de tirer parti de DMARC peuvent réduire considérablement la quantité de spam, de phishing et de courriels frauduleux, prétendant provenir d'ADP et délivrées dans les boîtes de réception des utilisateurs finaux.

Les organisations qui souhaitent profiter de la fiche DMARC d'ADP doivent mettre en œuvre des produits anti-spam ou anti-phishing spécifiques utilisant cette norme. Ces applications utiliseront le label DMARC d'ADP afin d'identifier et réduire le nombre de courriels frauduleux et de spam qu'une entreprise est amenée à recevoir. Pour plus d'informations techniques sur la mise en œuvre DMARC dans votre société, veuillez transmettre cette url à votre administrateur de serveur de messagerie : www.dmarc.org
Plus d'informations sur :
http://www.adp.com/who-we-are/data-security-and-privacy/protection-against-phishing.aspx#sthash.EOujoRpp.dpuf