

VPN SSL sans client ASA : Problèmes de plug-in RDP

Contenu

[Introduction](#)

[Informations générales](#)

[Plug-in Java](#)

[Plug-in Active-X](#)

[Plug-in RDP](#)

[Utilisation du plug-in RDP et RDP-2](#)

[Positionnement du client ActiveX contre Java](#)

[RDP-ActiveX](#)

[RDP-Java](#)

[Format de signet RDP](#)

[Plug-in RDP et équilibrage de charge VPN](#)

[FAQ](#)

[Pourquoi certains caractères tapés n'apparaissent-ils pas sur la session RDP distante ?](#)

[Problèmes connus avec les mappages de clavier](#)

[Le plug-in Java RDP peut-il prendre en charge les sessions RDP plein écran ?](#)

[Le client Java peut-il communiquer avec l'utilisation d'AES-256 pour le chiffrement ?](#)

[Dépannage des problèmes RDP](#)

[Caveats connus](#)

[Problèmes de mise à jour de la sécurité Microsoft](#)

[Client ActiveX](#)

[Client Java](#)

Introduction

Ce document fournit des réponses à certaines questions fréquemment posées au sujet du plug-in RDP (Remote Desktop Protocol), disponible pour les utilisateurs du VPN SSLVPN (Adaptive Security Appliance) de Cisco sans client.

Le plug-in RDP n'est qu'un des plug-ins disponibles pour les utilisateurs, ainsi que d'autres, tels que Secure Shell (SSH), Virtual Network Computing (VNC) et Citrix. Le plug-in RDP est l'un des plug-ins les plus utilisés dans cette collection. Ce document fournit plus de détails sur le déploiement et les procédures de dépannage de ce plug-in.

Note: Ce document ne fournit pas d'informations sur la configuration du plug-in RDP. Pour plus d'informations, reportez-vous au [Guide de déploiement VPN SSL Cisco ASA 5500, version 8.x](#).

Informations générales

Le plug-in RDP a évolué à partir d'un plug-in RDP basé uniquement sur Java, pour inclure à la fois le client RDP ActiveX (Internet Explorer) et le client Java (navigateurs non Internet Explorer).

Plug-in Java

Le client RDP Java utilise l'applet [RDP Java appropriée](#). L'applet Java est ensuite encapsulée dans un plug-in qui permet l'installation dans le portail sans client ASA.

Plug-in Active-X

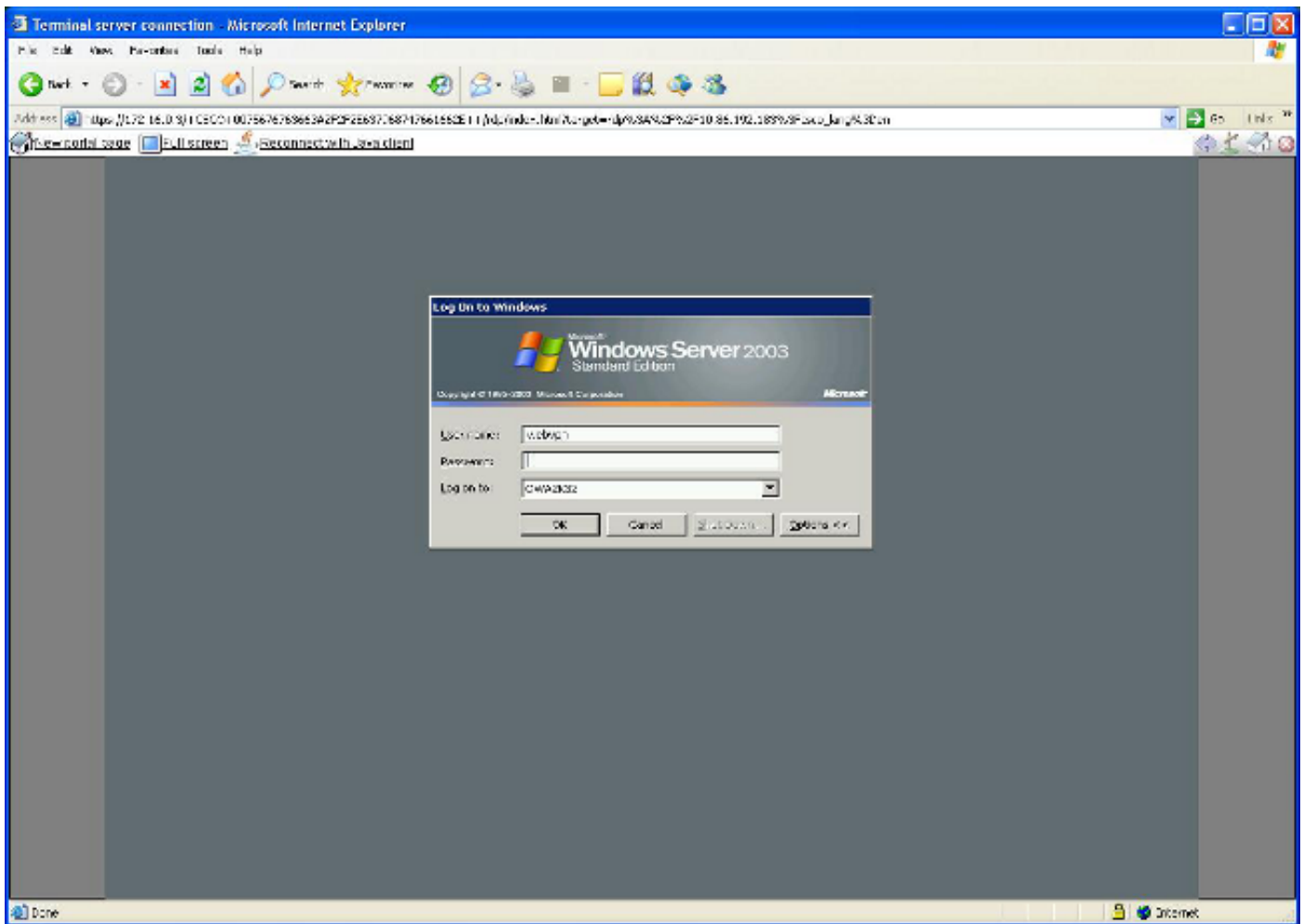
Le plug-in RDP inclut également le client RDP Microsoft ActiveX et le plug-in détermine s'il faut utiliser Java ou le client ActiveX en fonction du navigateur. C'est-à-dire :

- Si les utilisateurs d'Internet Explorer (IE) tentent d'utiliser RDP via un portail SSLVPN sans client et que l'URL du signet ne contient pas l'argument **ForceJava=true**, alors le client ActiveX est utilisé. Si ActiveX ne s'exécute pas, le plug-in initie le client Java.
- Si des utilisateurs non IE tentent de lancer un signet ou une URL RDP, seul le client Java est lancé.

Pour plus d'informations sur les conditions requises pour les privilèges RDP ActiveX et USER, reportez-vous à l'article [Configuration requise pour la connexion Web Bureau à distance](#).

L'image suivante illustre les trois liens qui peuvent être sélectionnés dans la fenêtre du navigateur après le lancement du plug-in :

1. **Nouvelle page du portail** - Ce lien ouvre la page du portail dans une nouvelle fenêtre de navigateur.
2. **Plein écran** - Utilise la fenêtre RDP en mode plein écran.
3. **Reconnexion avec Java** - Cela force le plug-in à se reconnecter et à utiliser Java au lieu d'ActiveX.



Plug-in RDP

Utilisation du plug-in RDP et RDP-2

- **Plug-in RDP** : Il s'agit du plug-in d'origine créé qui contient le client Java et ActiveX.
- **Plug-in RDP2** : En raison de modifications apportées au protocole RDP, le client RDP Java approprié a été mis à jour afin de prendre en charge les serveurs Terminal Server Microsoft Windows 2003 et les serveurs Terminal Server Windows Vista.

Astuce : Le dernier plug-in RDP combine les protocoles RDP et RDP2. Par conséquent, le plug-in RDP2 est obsolète. Il est recommandé d'utiliser la version la plus récente du plug-in RDP. Les nomenclatures du plug-in RDP suivent cette structure : **rdp-plugin.yyymmdd.jar**, où **yy** est un format d'année à deux chiffres, **mm** est un format de mois à deux chiffres, et **dd** est un format de jour à deux chiffres.

Pour télécharger le plug-in, visitez la [page de téléchargement de logiciels Cisco](#).

Worldwide [change] | Welcome, Adri Bessu | Account | Log Out | My Cisco

Products & Services | Support | How to Buy | Training & Events | Partners

Download Software

Download Cart (2 items) | Feedback | Help

Downloads Home > Products > Security > Firewalls > Firewall Appliances > Cisco ASA 5500 Series Adaptive Security Appliances > Cisco ASA 5520 Adaptive Security Appliance > Remote Access Plugins for Adaptive Security Appliance (ASA)-1.1.1

Download Path

Cisco ASA 5520 Adaptive Security Appliance

Search... | Expand All | Collapse All

All Releases

- 1.1.1
- 1.0.0

Release 1.1.1

File Information	Release Date	Size	
Terminal Service client plugin for ASA. rdp-plugin.120424.jar	27-APR-2012	0.86 MB	Download Add to cart Publish
Citrix (do-it-yourself) client plugin for ASA. ica-plugin.04.23.2012.zip	24-APR-2012	0.01 MB	Download Add to cart Publish
Cisco plugin for SiteMinder Policy Server to enable ASA SSO support via SiteMinder. cisco_vpn_auth.jar	15-FEB-2008	0.01 MB	Download Add to cart Publish
Citrix (do-it-yourself) client plugin for ASA. ica-plugin.100805.zip	15-FEB-2008	0.01 MB	Download Add to cart Publish
HTTP POST request plugin for ASA. post-plugin.090722.jar	15-FEB-2008	0.05 MB	Download Add to cart

Positionnement du client ActiveX contre Java

RDP-ActiveX

- Utilise IE uniquement
- Prise en charge du son transféré

RDP-Java

- Fonctionne sur tous les navigateurs pris en charge qui sont compatibles Java.
- Java Client est lancé dans IE uniquement si ActiveX ne démarre pas ou si l'argument **ForceJava=true** passe dans le signet RDP.
- L'implémentation RDP-Java est basée sur un projet RDP Java approprié, une initiative open source ; une assistance au mieux est fournie pour l'application.

Format de signet RDP

Voici un exemple de signet RDP :

```
rdp://server:port/?Parameter1=value&Parameter2=value&Parameter3=value
```

Voici quelques notes importantes sur le format :

- **server** - Il s'agit du seul attribut requis. Saisissez le nom de l'ordinateur qui héberge les services Terminal Server Microsoft.
- **port** (facultatif) : adresse virtuelle de l'ordinateur distant qui héberge les services Microsoft Terminal Server. La valeur par défaut, 3389, correspond au numéro de port connu de Microsoft Terminal Services.
- **settings** - Il s'agit d'une chaîne de requête facultative qui se compose de paires paramètre-valeur. Un point d'interrogation indique le début de la chaîne d'argument et chaque paire paramètre-valeur est séparée par une esperluette.

Voici une liste des paramètres disponibles :

géométrie : taille de l'écran client en pixels (L x H). **bpp** - Bits par pixel (profondeur de couleur), 8|16|24|32. **domain** - Il s'agit du domaine de connexion. **username** - Il s'agit du nom d'utilisateur pour la connexion. **password** : mot de passe de connexion. Utilisez le mot de passe avec soin, car il est utilisé côté client et peut être observé. **console** - Cette option est utilisée pour la connexion à la session de console sur le serveur (oui/non). **ForceJava** - Définissez ce paramètre sur **yes** afin d'utiliser uniquement le client Java. Le paramètre par défaut est **no**. **shell** - Définissez ce paramètre sur le chemin d'accès de l'exécutable/application qui est démarré automatiquement lorsque vous vous connectez au protocole RDP (**rdp://server/?shell=path**, par exemple).

Voici une liste de paramètres ActiveX uniquement supplémentaires :

RedirectDrives - Définissez ce paramètre sur **true** afin de mapper localement les lecteurs distants. **RedirectPrinters** - Définissez ce paramètre sur **true** afin de mapper localement les imprimantes distantes. **FullScreen** - Définissez ce paramètre sur **true** afin de le lancer en mode Plein écran. **ForceJava** - Définissez ce paramètre sur **yes** afin de forcer le client Java. **audio** - Ce paramètre est utilisé pour le transfert audio sur la session RDP :

0 - Redirige les sons distants vers l'ordinateur client. **1** - Lit des sons sur l'ordinateur distant. **2** - Désactive la redirection du son ; ne lit pas les sons sur le serveur distant.

Plug-in RDP et équilibrage de charge VPN

L'équilibrage de charge multi-géographie est pris en charge avec l'utilisation de l'[équilibrage de charge global du serveur](#) DNS (Domain Name Server). En raison des différences de mise en cache des résultats DNS, les plug-ins peuvent fonctionner différemment sur différents systèmes d'exploitation. Le cache DNS Windows permet au plug-in de résoudre la même adresse IP lorsqu'il lance l'applet Java. Sur Macintosh (MAC) OS X, il est possible que l'applet Java résolve une adresse IP différente. Par conséquent, le plug-in ne démarre pas correctement.

Un exemple de round-robin DNS est quand vous avez une URL unique (<https://www.example.com>) où l'entrée DNS pour **www.example.com** peut résoudre soit 192.0.2.10 (ASA1) soit 198.51.100.50 (ASA2).

Une fois que l'utilisateur s'est connecté au portail Client-WebVPN via un navigateur sur ASA1, il est possible d'initialiser le plug-in RDP. Au cours du lancement du client Java, les ordinateurs

MAC OS X exécutent une nouvelle demande de résolution DNS. Avec une configuration DNS circulaire, il y a 50 % de chance que cette réponse de seconde résolution retourne le même site que celui qui a été choisi pour la connexion WebVPN initiale. Si la réponse du serveur DNS est 198.51.100.50 (ASA2) plutôt que 192.0.2.10 (ASA1), le client Java initie une connexion à l'ASA (ASA2) incorrect. Comme la session utilisateur n'existe pas sur l'ASA2, la demande de connexion est rejetée.

Ceci peut entraîner des messages d'erreur Java similaires à ceci :

```
java.lang.ClassFormatError: Incompatible magic value 1008813135 in  
class file net/propero/rdp/applet/RdpApplet
```

FAQ

Pourquoi certains caractères tapés n'apparaissent-ils pas sur la session RDP distante ?

L'ordinateur distant de la session RDP peut avoir un paramètre de région du clavier différent de celui de l'ordinateur local. En raison de cette différence, il se peut que l'ordinateur distant n'affiche pas certains caractères tapés ou des caractères incorrects. Ce comportement n'est visible qu'avec le plug-in Java. Afin de résoudre ce problème, utilisez l'attribut **keymap** afin de mapper la clé locale dans le PC distant.

Par exemple, afin de définir un mappage de clavier allemand, utilisez :

```
rdp://
```

The following keymaps are available:

```
-----  
ar   de   en-us fi   fr-be it   lt   mk   pl   pt-br sl   tk  
da   en-gb es   fr   hr   ja   lv   no   pt   ru   sv   tr  
-----
```

Problèmes connus avec les mappages de clavier

- Identifiant de bogue Cisco CSCth38454 - Implémenter la clé hongroise pour le plug-in RDP.
- ID de bogue Cisco CSCsu77600 - Les clés de fenêtre du plug-in RDP WebVPN sont incorrectes. Maj (clé) .jar.
- ID de bogue Cisco CSCtt04614 - WebVPN - DIACRITIQUE DU clavier ES mal géré par le plug-in RDP.
- ID de bogue Cisco CSCtb07767 - Plugin ASA - Configurer les paramètres par défaut.

Astuce : Une autre solution possible consiste à utiliser un tunnel intelligent d'application pour

mstsc.exe. Ceci est configuré sous le mode de sous-configuration WebVPN avec cette commande : **fenêtres de plate-forme RDP_List RDP mstsc.exe smart-tunnel**.

Le plug-in Java RDP peut-il prendre en charge les sessions RDP plein écran ?

Actuellement, il n'existe aucune prise en charge native pour les sessions RDP plein écran. La demande d'amélioration CSCto87451 a été déposée afin de mettre en oeuvre ceci. Si le paramètre **géométrique** (**géométrie = 1024x768**, par exemple) est défini sur la résolution de l'écran de l'utilisateur, il fonctionne en mode plein écran. Étant donné que les tailles des écrans des utilisateurs varient, il peut être nécessaire de créer plusieurs liens de signet. Le client ActiveX prend nativement en charge les sessions RDP plein écran.

Le client Java peut-il communiquer avec l'utilisation d'AES-256 pour le chiffrement ?

Afin de permettre au client Java de négocier correctement le SSL, ajustez l'ordre du jeu de chiffrement SSL ASA pour qu'il corresponde à ceci :

```
Enabled cipher order: aes256-sha1 rc4-sha1 aes128-sha1 3des-sha1  
Disabled ciphers: des-sha1 rc4-md5 null-sha1
```

Le client Java peut afficher cette erreur si l'ordre du jeu de chiffrement est différent :

```
[Thread-12] INFO net.propero.rdp.Rdp - javax.net.ssl.SSLHandshakeException:  
Received fatal alert: handshake_failure
```

Dépannage des problèmes RDP

Si vous rencontrez d'autres problèmes avec le plug-in RDP, il peut être utile de collecter ces données afin de résoudre les problèmes RDP :

- La sortie **show tech** de l'ASA
- La sortie **détaillée du plug-in show import webvpn** de l'ASA
- Système d'exploitation et niveau de correctif de l'ordinateur utilisateur
- Système d'exploitation et niveau de correctif de l'ordinateur de destination
- Client utilisé (ActiveX ou Java) et version Java JRE
- Déterminer si l'ASA se trouve dans un cluster d'équilibrage de charge, basé sur DNS ou basé sur ASA

Caveats connus

Problèmes de mise à jour de la sécurité Microsoft

1. [KB2695962](#) - Avis de sécurité Microsoft : Mettre à jour le cumul pour les bits de terminaison ActiveX : 8 mai 2012.

2. [KB2675157](#) - MS12-023 : Mise à jour de sécurité cumulée pour Internet Explorer : 10 avril 2012.
3. [cisco-sa-20120314-asaclient](#) - Vulnérabilité à l'exécution de code à distance des dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500 VPN sans client ActiveX Control le 14 mars.
4. ID de bogue Cisco CSCtx68075 - Inversion ASA WebVPN lorsque le correctif Windows KB2585542 est appliqué (8.2.5.29 / 8.4.3.9).
5. [KB2585542](#) - MS12-006 : Description de la mise à jour de sécurité pour Webio, Winhttp et schannel dans Windows : 10 janvier 2012.

Client ActiveX

- **Symptômes** : Le client ActiveX ne parvient pas à se charger des versions 6 à 9 d'IE après une mise à niveau vers ASA OS version 8.4.3.

Reportez-vous à l'ID de bogue Cisco [CSCtx58556](#). Le correctif est disponible pour les versions 8.4.3.4 et ultérieures. Solution de contournement: Forcer l'utilisation du client Java.

- **Symptômes** : Le client ActiveX ne parvient pas à se charger après la rétrogradation de la version du système d'exploitation ASA vers une version antérieure à la version 8.4.3. Cela affecte les utilisateurs qui ont utilisé le client ActiveX sur un ASA avec la correction du bogue Cisco ID CSCtx58556, et se connectent à cet ASA avec une version antérieure à 8.4.3. Ceci est dû à un nouveau plug-in RDP ActiveX introduit dans ASA version 8.4.3, qui n'est pas compatible avec les versions précédentes.

Reportez-vous à l'ID de bogue Cisco CSCtx57453. Supprimer toutes les instances de Registre Windows de **b8e73359-3422-4384-8d27-4ea1b4c01232** ? (ancien CLSID ActiveX).

Note: Il est conseillé d'effectuer une sauvegarde du registre du système informatique avant toute modification.

- **Symptômes** : Les connexions RDP aux périphériques avec l'authentification au niveau du réseau (NLA) activée échouent.

Référez-vous à l'ID de bogue Cisco [CSCtu63661](#) pour l'amélioration qui demande à NLA d'être incorporé dans le plug-in ActiveX RDP. Bien que Microsoft ActiveX Client prenne en charge NLA, l'utilisation de cette fonctionnalité dans le plug-in ASA n'est pas prise en charge. Solution : configurez le plug-in RDP (**mstsc.exe**) pour qu'il soit doté d'un tunnel intelligent. Reportez-vous au [Guide de déploiement VPN SSL Cisco ASA 5500, version 8.x](#) .

- **Symptômes** : ActiveX RDP ne parvient pas à se charger et affiche une page vide.

Reportez-vous à l'ID de bogue Cisco [CSCsx49794](#). Cela se produit lorsque la chaîne de certificats pour le certificat SSL ASA est supérieure à quatre certificats (ROOT, SUBCA1, SUBCA2 et ASA CERT, par exemple). Solution de contournement:

N'installez pas la grande chaîne de certificats sur l'ASA. Le plug-in Java RDP fonctionne correctement, contrairement au plug-in ActiveX. RDP fonctionne également correctement

lorsque vous configurez Windows natif **mstsc.exe** avec des tunnels intelligents.

- **Symptômes** : Une fois le client RDP ActiveX utilisé, un utilisateur clique sur le bouton **Déconnexion** et reçoit une erreur **HTTP 404 - Page introuvable**. Reportez-vous à l'ID de bogue Cisco CSCtz33266. Ce problème est résolu avec le plug-in Version **rdp-plugin.120424.jar** ou ultérieur.
- **Symptômes** : Un utilisateur a deux onglets ouverts dans IE : un pour la session RDP et un autre pour une page Web vide ou autre. IE ne fonctionne pas correctement après la fermeture de l'onglet RDP.

Reportez-vous à l'ID de bogue Cisco [CSCua69129](#). Solution de contournement: Utilisez le plug-in Java RDP (Set **ForceJava=true**).

- **Symptômes** : Le plug-in ActiveX entraîne une utilisation élevée du CPU avec IE. Reportez-vous à l'ID de bogue Cisco [CSCua16597](#).
- **Symptômes** : Après l'installation de la mise à jour Windows **KB2695962**, le plug-in ActiveX RDP ne se charge pas. Lorsqu'une nouvelle session RDP est ouverte, le client ActiveX tente d'installer le **Cisco SSL VPN Port Forwarder** (ce qui n'est pas toujours le cas) et retourne à la page du portail sans client sans se connecter à l'ordinateur distant. Ceci est dû à la vulnérabilité **CVE-2012-0358**, qui est résolue côté client par [Microsoft Security Advisory \(2695962\)](#).

Référez-vous à Cisco Security Advisory [Cisco ASA 5500 Series Adaptive Security Appliance VPN sans client ActiveX Control Remote Code Execution Vulnerability](#). Reportez-vous à l'ID de bogue Cisco [CSCtr00165](#).

Client Java

Remarque : Cisco redistribue les plug-ins sans modification. En raison de la licence publique générale GNU, Cisco ne modifie ni n'étend l'application du plug-in. Le plug-in **JavaRDP approprié** est une application open source, et tout problème avec le logiciel du plug-in doit être traité par le propriétaire du projet.

- **Symptômes** : Les applications gourmandes en processeurs sont exécutées sur l'ordinateur distant lorsqu'elles sont accessibles via le client RDP Java, et un plantage d'applet Java se produit.

Ce message d'erreur peut s'afficher : **FATAL net.property.rdp - javax.net.ssl.SSLException : La connexion a été arrêtée** :Le comportement est déclenché lors de la commutation rapide entre deux applications gourmandes en CPU ou plus. Ce problème est corrigé dans les versions du plug-in **rdp.2012.6.4.jar** et ultérieures. Solution de contournement:

Se connecter à l'aide du client ActiveX. Ne passez pas rapidement d'une application à l'autre.

- **Symptômes** : Le client RDP Java génère ce message d'erreur : **net.property.rdp.Rdp -**

java.net.SocketException : Socket est fermé java.net.SocketException : Socket est fermé,
puis se ferme.

Le problème est causé par un groupe de tunnels qui a une url de groupe configurée avec uniquement le nom de domaine complet (FQDN) (http://www.example.com, par exemple).Référez-vous à l'ID de bogue Cisco [CSCuh72888](#).Solution de contournement:

Supprimez l'entrée group-URL sans "/" dans le groupe de tunnels.Utilisez le client ActiveX.

- **Symptômes** : Le client RDP Java échoue lorsqu'il est connecté à un ordinateur Windows 8.

Le client RDP Java n'est pas actuellement pris en charge pour cela.Reportez-vous à l'ID de bogue Cisco CSCuc79990Solution de contournement:

Utilisez le client RDP ActiveX.Tunnel intelligent du client RDP natif Windows (**mstsc.exe**).

- **Symptômes** : Le client RDP Java échoue avec ce message d'erreur : **ARSigningException : Entrée non signée trouvée dans la ressource :**
https://10.105.130.91/+CSCO+3a75676763663A2F2F2E637968747661662E++/vnc/VncViewer.jar.

Ce problème est causé par un bogue dans la réécriture Java WebVPN ASA.Reportez-vous à l'ID de bogue Cisco [CSCuj88114](#).Solution de contournement: Rétrograder vers Java Version 7u40.