

ASA clientloze SSLVPN: Plug-in problemen met RDP

Inhoud

[Inleiding](#)

[Achtergrondinformatie](#)

[Java-plug-in](#)

[Active-X plug-in](#)

[RDP-plug-in](#)

[Plug-in gebruik van RDP en RDP-2](#)

[ActiveX versus Java-clientpositie](#)

[RDP-actiefX](#)

[RDP-Java](#)

[RDP-favoriet](#)

[RDP plug-in en VPN-taakverdeling](#)

[FAQ's](#)

[Waarom verschijnen sommige getypte tekens niet op de afstandsbediening van RDP?](#)

[Bekende problemen met toetsenbordaangepassing](#)

[Kan de Java RDP-plug-in RDP-sessies op het volledige scherm ondersteunen?](#)

[Kan de Java-client communiceren met het gebruik van AES-256 voor codering?](#)

[Problemen oplossen](#)

[gekende Caveats](#)

[Problemen met Microsoft Security Update](#)

[ActiveX-client](#)

[Java-client](#)

Inleiding

Dit document geeft antwoorden op een aantal vaak gestelde vragen over de RDP-stekker (Remote Desktop Protocol), beschikbaar voor de gebruikers van Cisco adaptieve security applicatie (ASA) en clientloze Secure Socket Layer VPN (SSLVPN).

De RDP-plug-in is slechts een van de plug-ins die beschikbaar is voor gebruikers, in combinatie met andere functies zoals Secure Shell (SSH), Virtual Network Computing (VNC) en Citrix. De RDP-stekker is een van de meest gebruikte plug-ins in deze verzameling. Dit document bevat meer informatie over de implementatieprocedures en de procedures voor probleemoplossing voor deze plug-in.

Opmerking: Dit document bevat geen informatie over de manier waarop u de RDP-plug-in kunt configureren. Raadpleeg de [Cisco ASA 5500 SSL VPN-implementatiegids, versie 8.x](#) voor meer informatie.

Achtergrondinformatie

De RDP-plug-in is ontwikkeld van een pure Java-gebaseerde RDP-stekker, zodat deze zowel ActiveX RDP-client (Internet Explorer) als Java-client (browsers die niet-Internet Explorer zijn) omvat.

Java-plug-in

De Java RDP-client gebruikt de [juiste Java RDP](#)-applicatie. De Java-applet wordt dan verpakt in een stekker die installatie binnen het ASA-clientloze portaal mogelijk maakt.

Active-X plug-in

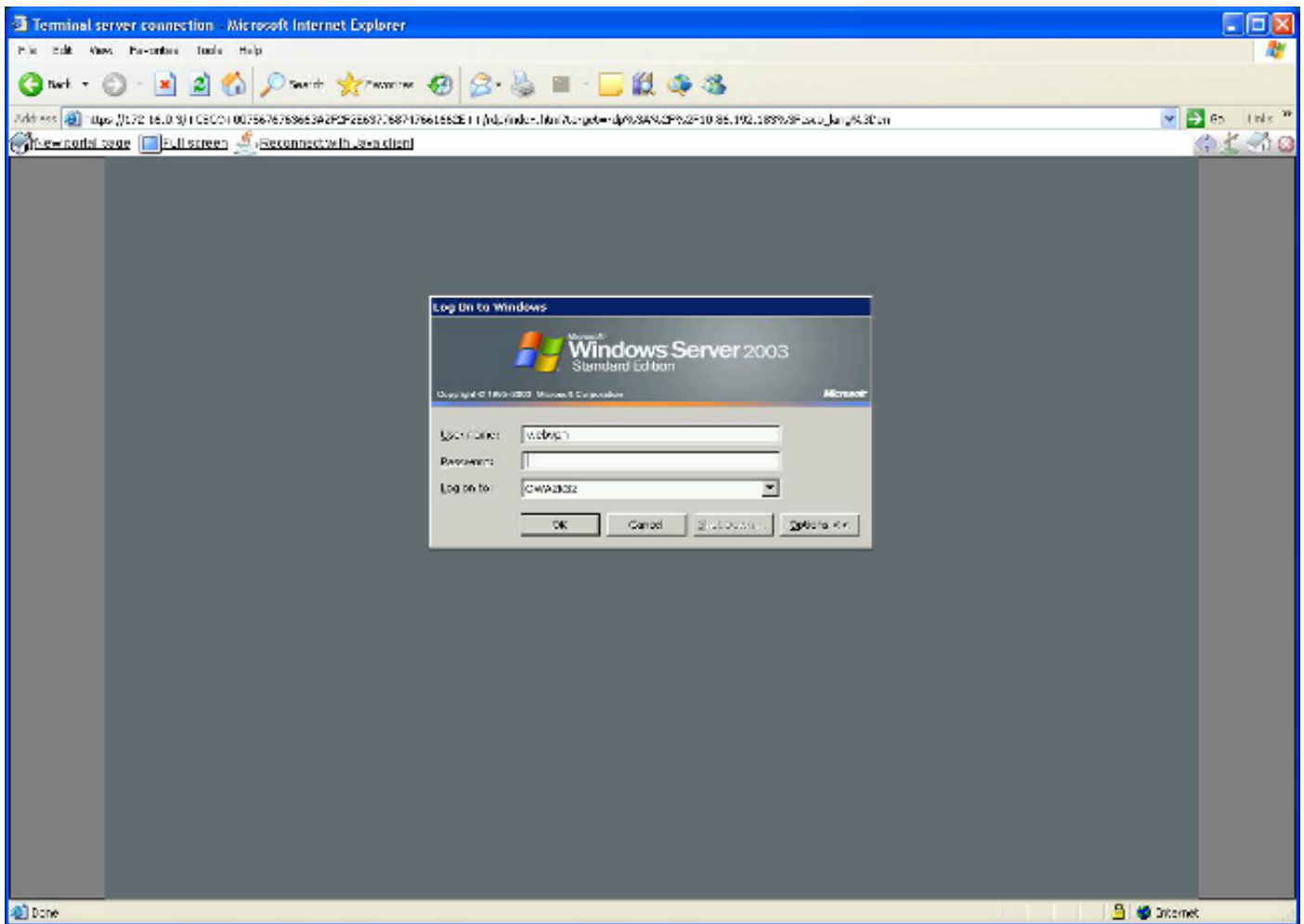
De RDP-plug-in bevat ook de Microsoft ActiveX RDP-client en de plug-in bepaalt of u Java of ActiveX-client wilt gebruiken op basis van de browser. Dat is:

- Als gebruikers van Internet Explorer (IE) proberen RDP te gebruiken via een Clientloos SSLVPN-portal en de favoriet-URL niet het **ForceJava=True**-argument bevat, dan wordt de ActiveX-client gebruikt. Als ActiveX niet wordt uitgevoerd, start de plug-in de Java-client.
- Als niet-IE gebruikers proberen een RDP-favoriet of URL te starten, wordt alleen de Java-client gestart.

Raadpleeg het artikel van de Microsoft [Requirements for Remote Desktop Web Connection](#) voor meer informatie over vereisten voor RDP ActiveX en USER-rechten.

De volgende afbeelding illustreert de drie koppelingen die binnen het browser venster kunnen worden geselecteerd nadat de plug-in is gestart:

1. **Nieuwe portal Pagina** - Deze link opent de portal pagina in een nieuw browser venster.
2. **Full-Screen** - Dit gebruikt het RDP-venster in de volledige schermmodus.
3. **Sluit opnieuw aan op Java** - Dit dwingt de stekker om Java opnieuw aan te sluiten en te gebruiken in plaats van ActiveX.



RDP-plug-in

Plug-in gebruik van RDP en RDP-2

- **RDP-plug-in:** Dit is de oorspronkelijke stekker die zowel Java als ActiveX-client bevat.
- **RDP2-plug-in:** Vanwege veranderingen in het RDP-protocol is de juiste Java RDP-client bijgewerkt ter ondersteuning van Microsoft Windows 2003 Terminalservers en Windows Vista-terminalservers.

Tip: De laatste RDP-plug-in combineert zowel RDP- als RDP2-protocollen. Als resultaat hiervan is de RDP2-plug-in verouderd. Aanbevolen wordt om de meest recente versie van de RDP-stekker te gebruiken. De nomenclatuur van de RDP-plug-in volgt deze structuur: **rdp-plugin.yymmdd.jar**, waarbij **yy** een jaarformaat met twee cijfers heeft, **mm** een maandformaat met twee cijfers en **dd** een dagformaat met twee cijfers.

Ga naar de [downloadpagina](#) van [Cisco-software](#) om de stekker te downloaden.

Worldwide [change] | Welcome, Adri Bess | 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

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

ActiveX versus Java-clientpositie

RDP-actiefX

- Alleen IE gebruiken
- Ondersteuning voor doorgestuurd geluid

RDP-Java

- Werkt aan alle ondersteunde browsers die Java-ingeschakeld zijn.
- Java-client wordt alleen gestart in IE als ActiveX niet is gestart of het argument **ForceJava=True** in de RDP-favoriet wordt doorgegeven.
- de RDP-Java-implementatie is gebaseerd op een passend Java-RDP-project, een open-sourcet-initiatief; er wordt voor de aanvraag de best mogelijke ondersteuning geboden.

RDP-favoriet

Hier is een voorbeeldformaat van een RDP-favoriet:

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

Hier volgen een paar belangrijke opmerkingen over de opmaak:

- **server** - Dit is de enige vereiste eigenschap. Voer de naam in van de computer waarop de Microsoft Terminal Services opgeslagen zijn.
- **poort** (optioneel) - Dit is het virtuele adres in de externe computer waarop de Microsoft Terminal Services worden gehuisvest. De standaardwaarde, 3389, past het bekende havenaantal voor de diensten van Microsoft Terminal aan.
- **parameters** - Dit is een optionele query string die bestaat uit parameter-waarde paren. Een vraagteken onderscheidt het begin van de argumentstring, en elk parameter-waarde paar wordt gescheiden door een ampersand.

Hier volgt een lijst met beschikbare parameters:

geometrie - Dit is de grootte van het clientscherm in pixels (W x H). **bpp** - Dit zijn de bits per pixel (kleurdiepte), 8|16|24|32. **domein** - Dit is het inlogdomein. **Gebruikersnaam** - Dit is de gebruikersnaam voor de inlognaam. **wachtwoord** - Dit is het inlogwachtwoord. Gebruik het wachtwoord voorzichtig, want het wordt gebruikt aan de kant van de client en kan worden waargenomen. **console** - Dit wordt gebruikt om verbinding te maken met de console-sessie op de server (ja/nee). **ForceJava** - Stel deze parameter in op **ja** om alleen de Java-client te gebruiken. De standaardinstelling is **nee**. **shell** - Stel deze parameter in op het pad van de uitvoerbaar/applicatie dat automatisch gestart wordt wanneer u verbinding maakt met RDP (**rdp://server/?shell=path**, bijvoorbeeld).

Hier is een lijst met extra parameters die alleen ActiveX bevatten:

RedirectDrives - Stel deze parameter in op **waar** om externe schijven lokaal in kaart te brengen. **RedirectPrinters** - Stel deze parameter in op **waarheid** om externe printers lokaal in kaart te brengen. **FullScreen** - Stel deze parameter in op **trouw** om deze in de modus FullScreen te starten. **ForceJava** - Stel deze parameter **ja in** om de Java-client te forceren. **audio**- Deze parameter wordt gebruikt voor audioverwerking tijdens de RDP-sessie:

0 - hiermee wordt het geluid van de afstandsbediening naar de clientcomputer omgeleid. **1** - Speelt geluid af op de afstandscomputer. **2** - maakt een gezonde omleiding uit; speelt geen geluid op de externe server.

RDP plug-in en VPN-taakverdeling

De taakverdeling voor meerdere geografie wordt ondersteund met gebruik van Domain Name Server (DNS)-gebaseerde [Global Server-taakverdeling](#). Als gevolg van verschillen in DNS-resultaat bij het opvangen van de resultaten, kunnen plug-ins verschillend werken in verschillende besturingssystemen. Windows DNS cache stelt de stekker in in in staat hetzelfde IP-adres op te lossen wanneer het wordt gestart met de Java-applet. Op Macintosh (MAC) OS X, is het mogelijk voor de Java-toets om een ander IP-adres op te lossen. Als resultaat hiervan is de plug-in niet correct gestart.

Een voorbeeld van DNS-round-robin is wanneer u één URL (<https://www.example.com>) hebt waar de DNS-ingang voor **www.example.com** ofwel 192.0.2.10 (ASA1) of 198.51.100.50 (ASA2) kan oplossen.

Nadat de gebruiker zich in het Clientless-WebVPN-portaal via een browser op ASA1 inlogt, is het starten van de RDP-plug-in mogelijk. Tijdens de start van de Java-client voeren MAC OS X-computers een nieuw DNS-afwikkelingsverzoek uit. Met een DNS-configuratie van een ronde band is er een kans van 50% dat deze tweede resolutie-respons dezelfde site teruggeeft die is geselecteerd voor de eerste WebVPN-verbinding. Als de DNS-serverrespons 198.51.100.50 (ASA2) is in plaats van 192.0.2.10 (ASA1), start de Java-client een verbinding met de verkeerde ASA2 (ASA2). Aangezien de gebruikerssessie niet op ASA2 bestaat, wordt het verbindingsverzoek verworpen.

Dit kan leiden tot Java-foutmeldingen die hier op lijken:

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

FAQ's

Waarom verschijnen sommige getypte tekens niet op de afstandsbediening van RDP?

De externe computer in de RDP-sessie kan een andere instelling voor een toetsenbord hebben dan de lokale computer. Als gevolg van dit verschil wordt bepaalde getypte tekens of onjuiste tekens mogelijk niet op de afstandscomputer weergegeven. Dit gedrag wordt alleen met de Java-instekker gezien. Om dit probleem op te lossen, gebruikt u de eigenschap **keymap** om de lokale toetsenbord in de afstandsbediening in kaart te brengen.

Bijvoorbeeld, om een Duits toetsenbord in kaart te brengen, gebruik:

```
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  
-----
```

Bekende problemen met toetsenbordaangepassing

- Cisco bug-ID CSCth38454 - Voer Hongaarse keymap voor RDP-stekker in.
- Cisco bug-ID CSCsu7600 - de toetsen in het venster voor WebVPN RDP-plug zijn onjuist. **Shift (toets) .jar**.
- Cisco bug-ID CSCt04614 - WebeVPN - ES-toetsenborddiakrieken die onjuist worden beheerd door RDP-stekker.
- Cisco bug-ID CSCtb0767 - ASA plug-in - standaardparameters configureren.

Tip: Een andere mogelijke oplossing is om een Application Smart Tunnel te gebruiken voor **mstsc.exe**. Dit wordt ingesteld onder de subconfiguratiemodus van WebVPN met deze opdracht: **smart-tunnellijst RDP_List RDP Mstsc.exe, platformvensters**.

Kan de Java RDP-plug-in RDP-sessies op het volledige scherm ondersteunen?

Op dit moment is er geen native ondersteuning voor RDP-sessies met het volledige scherm. Verbeteringsverzoek CSCto87451 is ingediend om dit te implementeren. Als de **geometrie** parameter (**geometrie=1024x768**, bijvoorbeeld) is ingesteld op de resolutie van de gebruikerspatroon, werkt deze in de volledige schermmodus. Aangezien de grootte van het gebruikersscherm varieert, kan het nodig zijn om meerdere favorietlinks te maken. De ActiveX-client ondersteunt RDP-sessies op het volledige scherm.

Kan de Java-client communiceren met het gebruik van AES-256 voor codering?

Om de Java-client in staat te stellen om de SSL correct te onderhandelen, stelt u de volgorde van de ASA SSL-algoritme in om dit aan te passen:

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

De Java-client kan deze fout weergeven als de volgorde van de cipherset anders is:

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

Problemen oplossen

Als u andere problemen ondervindt met de RDP-plug-in, kan het handig zijn om deze gegevens te verzamelen voor problemen bij de RDP-problemen:

- De **show tech**-uitvoer van de ASA
- De **show voert een gedetailleerde plug-in in** van de ASA-software
- Het besturingssysteem van de gebruikerscomputer en het patchniveau
- Besturingssysteem en patchniveau op de doelcomputer
- De client die wordt gebruikt (ActiveX of Java) en de Java JRE-versie
- Bepaal of de ASA in een belasting-balans cluster, DNS-gebaseerd of ASA-gebaseerd is

gekende Caveats

Problemen met Microsoft Security Update

1. [KB2695962](#) - Microsoft Security Advisory: Rollup bijwerken voor ActiveX Kill-bits: 8 mei 2012.

2. [B2675157](#) - MS12-023: Cumulatieve security update voor Internet Explorer: 10 april 2012.
3. [Cisco cisco-sa-20120314-poorts](#) - Cisco ASA 5500 Series adaptieve security applicatie zonder clientadaptieve VPN ActiveX Control Remote Code executie-mogelijkheid, 14 maart.
4. Cisco bug-ID CSCtx68075 - ASA WebVPN breken wanneer Windows Patch KB258542 wordt toegepast (8.2.5.29/8.4.3.9).
5. [B2585542](#) - MS12-006: Beschrijving van de beveiligingsupdate voor Webio, Winhttp en schannel in Windows: 10 januari 2012.

ActiveX-client

- **Symptomen:** ActiveX-client is niet geladen van IE versies 6 tot en met 9 na een upgrade naar ASA OS versie 8.4.3.

Raadpleeg Cisco bug-ID [CSCtx5856](#). De oplossing is beschikbaar voor versies 8.4.3.4 en hoger. Werken: Dwing het gebruik van de Java-client.

- **Symptomen:** ActiveX-client is niet geladen nadat de ASA OS-versie is gedowngraded naar een versie voorafgaand aan 8.4.3. Dit beïnvloedt gebruikers die de ActiveX-client in een ASA hebben gebruikt met de oplossing voor Cisco bug ID CSCtx5856 en sluit deze ASA aan op een versie voorafgaand aan 8.4.3. Dit is te wijten aan een nieuwe ActiveX RDP-plug-in ASA versie 8.8 4.3, hetgeen niet verenigbaar is met de eerdere versies.

Raadpleeg Cisco bug-ID CSCtx57453. Verwijder alle Windows-registratiefasen van **b8e73359-3422-4384-8d27-4ea1b4c01232?** (oude ActiveX CLSID).

Opmerking: Aanbevolen wordt om een back-up van het computersysteemregister uit te voeren voordat er wijzigingen in worden aangebracht.

- **Symptomen:** RDP-verbindingen met apparaten die zijn ingeschakeld met Network Level Authentication (NLA).

Raadpleeg Cisco bug-ID [CSCtu63661](#) voor de verbetering waarvoor NLA gevraagd wordt om ingebouwd te worden in de ActiveX RDP-stekker. Hoewel Microsoft ActiveX Client NLA ondersteunt, wordt het gebruik van deze functie in de ASA plug-in niet ondersteund. Workround: configureren van de RDP plug-in (**mstsc.exe**) om slim-afgestemd te worden. Raadpleeg de [Cisco ASA 5500 SSL VPN Deployment Guide, versie 8.x](#).

- **Symptomen:** ActiveX RDP kan niet worden geladen en toont een lege pagina.

Raadpleeg Cisco bug-ID [CSCsx49794](#). Dit gebeurt wanneer de certificeringsketen voor het ASA SSL-certificaat groter is dan vier certificaten (ROOT, SUBCA1, SUBCA2 en ASA CERT, bijvoorbeeld). Werken:

Installeer de grote certificeringsketen niet op de ASA. Het is bekend dat de Java RDP-plug-in correct werkt in tegenstelling tot de ActiveX-stekker. RDP werkt ook correct als u het oorspronkelijke Windows **mstsc.exe** configureren met slimme tunnels.

- **Symptomen:** Nadat de ActiveX RDP-client is gebruikt, klikt een gebruiker op de **Uitlogknop** en

ontvangt hij een **HTTP 404 - Page Not found** error. Raadpleeg Cisco bug-ID CSCtz3266. Dit probleem is opgelost met plug-in versie **rdp-plug-in.120424.jar** of hoger.

- **Symptomen:** Een gebruiker heeft twee tabbladen open in IE - een voor de RDP-sessie en een ander voor een lege of andere webpagina. IE werkt niet correct nadat het tabblad RDP is gesloten.

Raadpleeg Cisco bug-ID [CSCua69129](#).Werken: Gebruik de Java RDP-plug-in (Stel **ForceJava=True**) in.

- **Symptomen:** De ActiveX-plug-in veroorzaakt gebruik met hoge CPU's bij IE. Raadpleeg Cisco bug-ID [CSCua16597](#).
- **Symptomen:** Na de installatie van de Windows-update **KB2695962** wordt de ActiveX RDP-plug-in niet geladen. Wanneer een nieuwe RDP-sessie wordt geopend, probeert de ActiveX-client de **Cisco SSL VPN-poortadapter** te installeren (dit gebeurt niet altijd) en keert deze terug naar de clientloze portal-pagina zonder verbinding met de externe computer. Dit is te wijten aan kwetsbaarheid **CVE-2012-0358**, die aan de cliënt door [Microsoft Security Advisory \(2695962\)](#) wordt opgelost.

Raadpleeg Cisco Security Adviserende [Cisco ASA 5500 Series adaptieve security applicatie zonder client VPN ActiveX Control Remote Code executie-kwetsbaarheid](#).Raadpleeg Cisco plug-in [CSCtr00165](#).

Java-client

Opmerking: Cisco herdistribueert plug-ins zonder veranderingen. Als gevolg van de GNU General Public License, verandert Cisco de plug-in toepassing niet en breidt deze niet uit. De **juiste** JavaRDP-stekker is een open-source toepassing en alle problemen met de plug-in-software moeten door de eigenaar van het project worden aangepakt.

- **Symptomen:** processorintensieve toepassingen worden op de afstandscomputer uitgevoerd wanneer ze via de Java RDP-client worden benaderd, en een Java Applet-crash wordt ervaren.

Dit foutbericht kan worden weergegeven: **FATAL net.Properties.rdp - javax.net.ssl.SSLExeption: Verbinding is afgesloten:**Het gedrag wordt geactiveerd wanneer snel wordt overgeschakeld tussen twee of meer CPU-intensieve toepassingen.Dit probleem wordt vastgesteld in de plug-in versies rdp.2012.6.4.jar en hoger. Werken:

Connect met gebruik van de ActiveX-client.Switch niet snel tussen de applicaties.

- **Symptomen:** De Java RDP-client genereert deze foutmelding: **net..propo.rdp.rdp - java.net.SoraketException: Socket is gesloten java.net.SoketException: Socket is gesloten**, en dan sluit.

Het probleem wordt veroorzaakt door een tunnel-groep die een groep-url heeft die met slechts

de FQDN (<http://www.example.com>, bijvoorbeeld) wordt gevormd. Raadpleeg Cisco bug-ID [CSC7288](#). Werken:

Verwijder de groep-URL ingang zonder een "/" in de tunnelgroep. Gebruik de ActiveX-client.

- **Symptomen:** Java RDP-client mislukt wanneer deze is aangesloten op een Windows 8-computer.

De Java RDP-client heeft hier momenteel geen ondersteuning voor. Raadpleeg Cisco bug-id [CSCuc7990](#) Werken:

Gebruik de ActiveX RDP-client. Smart-tunnel op de oorspronkelijke RDP-client (**mstsc.exe**).

- **Symptomen:** De Java RDP-client heeft deze foutmelding niet: **ABBYigningException: Vond niet-ondertekende vermelding in middelen:**
<https://10.105.130.91/+CSCO+3a75676763663A2F2F2E637968747661662E++/vnc/VncViewer.jar>.

Dit probleem wordt veroorzaakt door een bug in de ASA webVPN Java rewriter. Raadpleeg Cisco bug-ID [CSCuj8114](#). Werken: Downgrade naar Java versie 7u40.