# ASA Clientless SSLVPN: RDP Plug-in Issues

## Contents

## Introduction

This document provides answers to some frequently asked questions about the Remote Desktop Protocol (RDP) plug-in, available to Cisco Adaptive Security Appliance (ASA) Clientless Secure Sockets Layer VPN (SSLVPN) users.

The RDP plug-in is only one of the plug-ins available to users, along with others such as Secure Shell (SSH), Virtual Network Computing (VNC), and Citrix. The RDP plug-in is one of the most frequently used plug-ins in this collection. This document provides more details about the deployment and troubleshoot procedures for this plug-in.

> **Note**: This document does not provide information about how to configure the RDP plug-in. For additional information, refer to the Cisco ASA 5500 SSL VPN Deployment Guide, Version 8.x.

## Background Information

The RDP plug-in has evolved from a pure Java-based RDP plug-in, to include both ActiveX RDP Client (Internet Explorer), as well as Java Client (Non-Internet Explorer browsers).

### Java Plug-In

The Java RDP Client utilizes the Proper Java RDP applet. The Java applet is then wrapped within a plug-in that allows installation within the ASA clientless portal.

### Active-X Plug-In

The RDP plug-in also includes the Microsoft ActiveX RDP Client, and the plug-in determines whether to use Java or ActiveX Client based on the browser. That is:

- If Internet Explorer (IE) users attempt to use RDP through a Clientless SSLVPN Portal, and the bookmark URL does not contain the **ForceJava=true** argument, then the ActiveX Client is used. If ActiveX fails to execute, the plug-in initiates the Java client.
- If non-IE users attempt to launch an RDP bookmark or URL, only the Java Client is launched.

For more information on requirements for RDP ActiveX and USER privileges, reference the Microsoft Requirements for Remote Desktop Web Connection article.

The next image illustrates the three links that can be selected within the browser window after the plug-in is launched:

1. **New Portal Page** - This link opens the portal page in a new browser window.
2. **Full-Screen** - This uses the RDP window in full-screen mode.
3. **Reconnect with Java** - This forces the plug-in to reconnect and use Java instead of ActiveX.

## RDP Plug-In

### RDP and RDP-2 Plug-In Usage

- **RDP plug-in:** This is the original plug-in created that contains both the Java and ActiveX Client.
- **RDP2 plug-in:** Due to changes within the RDP protocol, the Proper Java RDP Client was updated in order to support Microsoft Windows 2003 Terminal Servers and Windows Vista Terminal Servers.

> **Tip**: The latest RDP plug-in combines both RDP and RDP2 protocols. As a result the RDP2 plug-in is obsolete. It is recommended to utilize the most-recent version of the RDP plug-in. The RDP plug-in nomenclatures follows this structure: **rdp-plugin.yymmdd.jar**,where **yy** is a two-digit year format, **mm** is a two-digit month format, and **dd** is a two-digit day format.

In order to download the plug-in, visit the Cisco software download page.

## ActiveX Versus Java Client Positioning

### RDP-ActiveX

- Uses IE only
- Provides support for forwarded sound

### RDP-Java

- Works on all supported browsers that are Java-enabled.
- Java Client is launched in IE only if ActiveX fails to launch, or the **ForceJava=true** argument passes in the RDP bookmark.
- RDP-Java implementation is based on Proper Java RDP project, an open-source initiative; best-effort support is provided for the application.

## RDP Bookmark Format

Here is an example format of an RDP bookmark:

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

Here are some important notes about the format:

- **server** - This is the only required attribute. Enter the name of the computer that hosts the Microsoft Terminal Services.
- **port** (optional) - This is the virtual address within the remote computer that hosts the Microsoft Terminal Services. The default value, 3389, matches the well-known port number for Microsoft Terminal Services.
- **parameters** - This is an optional query string that consists of parameter-value pairs. A question mark demarks the beginning of the argument string, and each parameter-value pair is separated by an ampersand.

  Here is a list of available parameters:

  **geometry** - This is the size of the client screen in pixels (W x H).**bpp** - This is the bits-per-pixel (color depth), 8|16|24|32.**domain** - This is the login domain.**username** - This is the username for login.**password** - This is the login password. Use the password with care, because it is used at the client-side and can be observed.**console** - This is used in order to connect to the console session on the server (yes/no).**ForceJava** - Set this parameter to **yes** in order to use only the Java Client. The default setting is **no**.**shell** - Set this parameter to the path of the executable/application that is started automatically when you connect with RDP (**rdp://server/?shell=path**, for example).

Here is a list of additional ActiveX-only parameters:

**RedirectDrives** - Set this parameter to **true** in order to map remote drives locally.**RedirectPrinters** - Set this parameter to **true** in order to map remote printers locally.**FullScreen -** Set this parameter to **true** in order to launch in FullScreen mode.**ForceJava** - Set this parameter to **yes** in order to force the Java Client**.audio**- This parameter is used for audio forwarding over the RDP session:

**0** - Redirects remote sounds to the client computer.**1** - Plays sounds at the remote computer.**2** - Disables sound redirection; does not play sounds at the remote server.

## RDP Plug-In and VPN Load-Balancing

Multi-geography load-balancing is supported with use of Domain Name Server (DNS)-based Global Server Load Balancing. Due to DNS result caching differences, plug-ins might operate differently across varied operating systems. Windows DNS cache allows the plug-in to resolve the same IP address when it lauches the Java applet. On Macintosh (MAC) OS X, it is possible for the Java applet to resolve a different IP address. As a result, the plug-in fails to launch correctly.

An example of DNS round-robin is when you have a single URL (https://www.example.com) where the DNS entry for **www.example.com** can resolve either 192.0.2.10 (ASA1) or 198.51.100.50 (ASA2).

After the user logs into the Clientless-WebVPN portal via a browser on ASA1, initiaition of the RDP plug-in is possible. During the initiation of the Java client, MAC OS X computers execute a new DNS resolution request. With a round-robin DNS configuration, there is a 50% chance that this second resolution response returns the same site that was chosen for the initial WebVPN connection. If the DNS server response is 198.51.100.50 (ASA2) rather than 192.0.2.10 (ASA1), the Java client initiates a connection to the wrong ASA (ASA2). As the user session does not exist on the ASA2, the connection request is rejected.

This might result in Java error messages similar to this:

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

# FAQs

## Why do some typed characters not appear on the remote RDP session?

The remote computer in the RDP session might have a different keyboard region setting than the local computer. Due to this difference, the remote computer might not display certain typed characters or incorrect characters. This behavior is seen with only with the Java plug-in. In order to resolve this problem, use the **keymap** attribute in order to map the local keymap into the remote PC.

For example, in order to set a German keyboard mapping, use:

```
rdp://<IP Address of the server>/?keymap=de

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
---------------------------------------------------------------------
```

### Known Issues with Keyboard Mappings

- Cisco bug ID CSCth38454 - **Implement Hungarian keymap for RDP plug-in.**
- Cisco bug ID CSCsu77600 - **WebVPN RDP plugin window keys are incorrect. Shift (key) .jar**.
- Cisco bug ID CSCtt04614 - **WebVPN - ES keyboard diacritics incorrectly managed by RDP plugin.**
- Cisco bug ID CSCtb07767 - **ASA Plugin - Configure default parameters**.

**Tip**: Another possible workaround is to use an Application Smart Tunnel for **mstsc.exe.** This is configured under the WebVPN sub-configuration mode with this command: **smart-tunnel list RDP_List RDP mstsc.exe platform windows**.

## Can the Java RDP plug-in support full-screen RDP sessions?

Currently, there is no native support for full-screen RDP sessions. Enhancement request CSCto87451 was filed in order to implement this. If the **geometry** parameter (**geometry =1024x768**, for example) is set to the resolution of the user monitor, it operates in full-screen mode. As user screen sizes vary, it might be necessary to create multiple bookmark links. The ActiveX client natively supports full-screen RDP sessions.

## Can the Java client communicate with use of AES-256 for encryption?

In order to allow the Java client to negotiate the SSL correctly, adjust the order of the ASA SSL cipher-set to match this:

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

The Java client might display this error if the cipher-set order is different:

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

# Troubleshoot RDP Issues

If you experiences other issues with the RDP plug-in, it might be useful to Collect this data in order to troubleshoot RDP issues:

- The **show tech** output from the ASA
- The **show import webvpn plug-in detailed** output from the ASA
- The user computer Operating System and patch-level
- The destination computer Operating System and patch-level
- The client that is used (ActiveX or Java) and Java JRE version
- Determine if the ASA is in a load-balance cluster, DNS-based, or ASA-based

# Known Caveats

## Microsoft Security Update Issues

1. KB2695962 - Microsoft Security Advisory: Update Rollup for ActiveX Kill Bits: May 8, 2012.
2. KB2675157 - MS12-023: Cumulative Security Update for Internet Explorer: April 10, 2012.
3. cisco-sa-20120314-asaclient - Cisco ASA 5500 Series Adaptive Security Appliance Clientless VPN ActiveX Control Remote Code Execution Vulnerability March 14th.
4. Cisco bug ID CSCtx68075 - ASA WebVPN breaking when Windows Patch KB2585542 is applied (8.2.5.29 / 8.4.3.9).
5. KB2585542 - MS12-006: Description of the security update for Webio, Winhttp, and schannel in Windows: January 10, 2012.

## ActiveX Client

- **Symptoms**: ActiveX Client fails to load from IE Versions 6 through 9 after an upgrade to ASA OS Version 8.4.3.

  Refer to Cisco bug ID CSCtx58556. The fix is available for Versions 8.4.3.4 and later.Workaround: Force the use of the Java Client.

- **Symptoms**: ActiveX Client fails to load after the ASA OS Version is downgraded to a version prior to 8.4.3. This affects users that have used the ActiveX client on an ASA with the fix for Cisco bug ID CSCtx58556, and connect to this ASA with a version prior to 8.4.3. This is due to a new ActiveX RDP plug-in introduced in ASA Version 8.4.3, which is not compatible with the earlier versions.

  Refer to Cisco bug ID CSCtx57453.Remove all Windows registry instances of **b8e73359-3422-4384-8d27-4ea1b4c01232?** (old ActiveX CLSID).

  **Note**: It is suggested to perform a backup of the computer system registry prior to any edits.
- **Symptoms**: RDP connections to devices with Network Level Authentication (NLA) enabled fail.

  Refer to Cisco bug ID CSCtu63661 for the enhancement that requests NLA to be incorporated within the ActiveX RDP plug-in.Although Microsoft ActiveX Client supports NLA, use of that feature within the ASA plug-in is not supported.Workaround: Configure the RDP plug-in (**mstsc.exe**) to be smart-tunnelled. Refer to Cisco ASA 5500 SSL VPN Deployment Guide, Version 8.x .

- **Symptoms**: ActiveX RDP fails to load, and shows a blank page.

  Refer to Cisco bug ID CSCsx49794.This occurs when the certificate chain for the ASA SSL certificate is greater than four certificates (ROOT, SUBCA1, SUBCA2, and ASA CERT, for example).Workaround:

  Do not install the large certificate chain on the ASA.Java RDP plug-in is known to work properly, as opposed to the ActiveX plug-in.RDP also works properly when you configure native Windows **mstsc.exe** with smart tunnels.

- **Symptoms**: After the ActiveX RDP Client is used, a user clicks the **Logout** button and receives an **HTTP 404 - Page Not found** error. Refer to Cisco bug ID CSCtz33266. This issue has is resolved with plug-in Version **rdp-plugin.120424.jar** or later.

- **Symptoms**: A user has two tabs open in IE - one for the RDP session and another for a blank or other webpage. IE fails to operate correctly after the RDP tab is closed.

  Refer to Cisco bug ID CSCua69129.Workaround: Use the Java RDP plug-in (Set **ForceJava=true**).

- **Symptoms**: The ActiveX plug-in causes high-CPU usage with IE. Refer to Cisco bug ID CSCua16597.

- **Symptoms**: After installation of Windows update **KB2695962,** the ActiveX RDP plug-in does not load. When a new RDP session is opened, the ActiveX client attempts to install the **Cisco SSL VPN Port Forwarder** (this does not always happen) and returns to the clientless portal page without connecting to the remote computer. This is due to vulnerability **CVE-2012-0358,** which is resolved on the client-side by Microsoft Security Advisory (2695962).

  Refer to Cisco Security Advisory Cisco ASA 5500 Series Adaptive Security Appliance Clientless VPN ActiveX Control Remote Code Execution Vulnerability.Refer to Cisco Bug ID CSCtr00165.

## Java Client

**Note**: Cisco redistributes plug-ins without any changes. Due to GNU General Public License, Cisco does not alter or extend the plug-in application. The **properJavaRDP** plug-in is an open-source application, and any issues with the plug-in software must be addressed by the project owner.

- **Symptoms**: Processor-intensive applications are run on the remote computer when accessed via the Java RDP Client, and a Java Applet crash is experienced.

This error message might display: **FATAL net.propero.rdp  - javax.net.ssl.SSLException: Connection has been shutdown: .....**The behavior is triggerd when switching between two or more CPU-intensive applications rapidly.This Issue is fixed in plug-in Versions rdp.2012.6.4.jar and later. Workaround:

Connect with use of the ActiveX Client.Do not switch between applications rapidly.

- **Symptoms**: The Java RDP Client generates this error message: **net.propero.rdp.Rdp - java.net.SocketException: Socket is closed java.net.SocketException: Socket is closed**, and then closes.

  The issue is caused by a tunnel-group that has a group-url configured with only the FQDN (http://www.example.com, for example).Refer to Cisco bug ID CSCuh72888.Workaround:

  Remove the group-URL entry without a "/" in the tunnel-group.Use the ActiveX Client.

- **Symptoms**: Java RDP Client fails when it is connected to a Windows 8 computer.

  The Java RDP Client does not currently have support for this.Refer to Cisco bug ID CSCuc79990Workaround:

  Use the ActiveX RDP Client.Smart tunnel the Windows native RDP client (**mstsc.exe**).

- **Symptoms**: The Java RDP Client fails with this error message: **ARSigningException: Found unsigned entry in resource: https://10.105.130.91/+CSCO+3a75676763663A2F2F2E637968747661662E++/vnc/VncViewer.jar**.

  This issue is caused by a bug in the ASA webVPN Java rewriter.Refer to Cisco bug ID CSCuj88114.Workaround: Downgrade to Java Version 7u40.