



# Accessing Remote Desktop using VNC on Dell PowerEdge Servers

Establish secure remote desktop connections to Server Host OS using standard VNC clients, starting iDRAC7 firmware version 1.50.50

Harsha S Biradar  
Rajesh Z Patel  
Chetan S Deshmukh  
David Warden

April 2015



THIS WHITE PAPER IS FOR INFORMATIONAL PURPOSES ONLY, AND MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, WITHOUT EXPRESS OR IMPLIED WARRANTIES OF ANY KIND.

© 2015 Dell Inc. All rights reserved. Reproduction of this material in any manner whatsoever without the express written permission of Dell Inc. is strictly forbidden. For more information, contact Dell.

PRODUCT WARRANTIES APPLICABLE TO THE DELL PRODUCTS DESCRIBED IN THIS DOCUMENT MAY BE FOUND AT: <http://www.dell.com/learn/us/en/19/terms-of-sale-commercial-and-public-sector> Performance of network reference architectures discussed in this document may vary with differing deployment conditions, network loads, and the like. Third party products may be included in reference architectures for the convenience of the reader. Inclusion of such third party products does not necessarily constitute Dell's recommendation of those products. Please consult your Dell representative for additional information.

Trademarks used in this text:

Dell™, the Dell logo, Dell Boomi™, Dell Precision™, OptiPlex™, Latitude™, PowerEdge™, PowerVault™, PowerConnect™, OpenManage™, EqualLogic™, Compellent™, KACE™, FlexAddress™, Force10™ and Vostro™ are trademarks of Dell Inc. Other Dell trademarks may be used in this document. Cisco Nexus®, Cisco MDS®, Cisco NX-OS®, and other Cisco Catalyst® are registered trademarks of Cisco System Inc. EMC VNX®, and EMC Unisphere® are registered trademarks of EMC Corporation. Intel®, Pentium®, Xeon®, Core® and Celeron® are registered trademarks of Intel Corporation in the U.S. and other countries. AMD® is a registered trademark and AMD Opteron™, AMD Phenom™ and AMD Sempron™ are trademarks of Advanced Micro Devices, Inc. Microsoft®, Windows®, Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista® and Active Directory® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Red Hat® and Red Hat® Enterprise Linux® are registered trademarks of Red Hat, Inc. in the United States and/or other countries. Novell® and SUSE® are registered trademarks of Novell Inc. in the United States and other countries. Oracle® is a registered trademark of Oracle Corporation and/or its affiliates. Citrix®, Xen®, XenServer® and XenMotion® are either registered trademarks or trademarks of Citrix Systems, Inc. in the United States and/or other countries. VMware®, Virtual SMP®, vMotion®, vCenter® and vSphere® are registered trademarks or trademarks of VMware, Inc. in the United States or other countries. IBM® is a registered trademark of International Business Machines Corporation. Broadcom® and NetXtreme® are registered trademarks of Broadcom Corporation. Qlogic is a registered trademark of QLogic Corporation. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and/or names or their products and are the property of their respective owners. Dell disclaims proprietary interest in the marks and names of others.



# Table of contents

Executive summary .....	4
1 Introduction .....	5
1.1 System Requirements.....	5
2 Configuring VNC Server on iDRAC.....	6
2.1 Using GUI.....	6
2.2 Using RACADM .....	8
3 Establishing VNC connection using <i>RealVNC</i> VNC Client on Windows OS.....	11
3.1 Installing RealVNC.....	11
3.2 Connecting Using RealVNC without SSL.....	11
3.2.1 Configuring iDRAC VNC Server for unencrypted VNC connection .....	11
3.2.2 Configuring RealVNC Client .....	11
3.3 Connecting Using RealVNC over SSL, using <i>ssltunnel</i> .....	14
3.3.1 Configuring iDRAC VNC Server for encrypted VNC connection.....	14
3.3.2 Installing and configuring 'ssltunnel' application .....	14
3.3.3 Configuring RealVNC Client to connect through SSL tunnel.....	15
4 Connecting securely with <i>SSVNC</i> Client on Windows .....	18
4.1 Installing <i>SSVNC</i> .....	18
4.2 Connecting Using <i>SSVNC</i> .....	18
5 Connecting with <i>bVNC</i> Client on Android.....	22
5.1 Installing <i>bVNC</i> .....	22
5.2 Connecting using <i>bVNC</i> .....	23
6 Accessing Virtual Media with VNC Session .....	25
6.1 Launching Virtual Media .....	25
6.2 Mapping Virtual Media.....	26
6.3 UnMapping Virtual Media .....	29
7 Troubleshooting.....	30



## Executive summary

Improved efficiency and security are always on top of the IT Admin requirements list. Dell's 12<sup>th</sup> and 13<sup>th</sup> generation PowerEdge servers and later have embedded management tools that meet the ever demanding challenges. The Remote Desktop feature on PowerEdge Servers is powered by iDRAC ( integrated Dell Remote Access Controller ) through proprietary Virtual Console, which has its own limitations with respect to performance and ease of use. To overcome, Virtual Network Computing (VNC) technology is now incorporated in iDRAC Enterprise firmware, starting version 1.50.50 , available with Enterprise License.

With VNC server enabled on iDRAC, IT admins can easily and securely access the operating system running on the server using a VNC client. The VNC client can be on any device – desktop, laptop, tablet, or phone – providing access from anywhere to quickly mitigate any issues or make changes to the OS. VNC clients implement the Remote Framebuffer (RFB) protocol to communicate with remote VNC server. For greater security, the connection can be made using a secure SSL based tunnel.

This document describes how to enable VNC support on iDRAC and securely connect using clients on Microsoft Windows and Android platforms.



# 1 Introduction

Remote desktop connections to Server Host OS are useful in debugging issues when OS/Servers in DataCenters stops functioning in desirable manner. Monitoring consoles get alerts for such issues, and in turn send email or SMS alerts to mobile device with details to launch VNC session, giving access to OS/Hypervisor on server and access to connected keyboard ,video and mouse, to take corrective actions, including OS reboot or similar.

On Dell PowerEdge Servers, remote desktop feature is enabled using Proprietary feature called Virtual Console on iDRAC, accessible only through iDRAC web interface, and dependent on either vulnerable ActiveX in IE browser or Java applet using Java environment, when using other browsers like Firefox or Chrome. It also means no standard client can be used to connect to remote desktop.

With iDRAC VNC (Virtual Network Computing) Server enabled on iDRAC, user gets a convenient way to establish remote desktop sessions independent of the host operating system, using a standard, thin and open VNC client. For security reasons, it is recommended that VNC sessions be secured using a Transport Layer Security/Secure Sockets Layer (TLS/SSL) tunnel. This best practices guide describes how to configure iDRAC VNC support for optimal performance and security.

VNC clients are available for a variety of desktop and mobile platforms. This document explains how to establish a connection from VNC clients with integrated support for iDRAC-compatible TLS/SSL tunnels on the Android and Microsoft Windows platforms.

iDRAC allows establishing either VNC session or Virtual Console session at any given time but only one VNC session is allowed at any given time.

Virtual Media feature is available in both session types. If a VNC session is active, you can only launch the Virtual Media using Launch Virtual Console and not the Virtual Console Viewer, explained in detail in [section 6](#).

## 1.1 System Requirements

iDRAC VNC Support requires the following:

- A 12<sup>th</sup> generation or later Dell PowerEdge server (with iDRAC7 or later)
- iDRAC firmware version 1.50.50 or later.
- All 13<sup>th</sup> or greater generation servers will have updated firmware.

**Note:** For information on applying iDRAC7 firmware updates see the white paper located at: [http://en.community.dell.com/techcenter/extras/m/white\\_papers/20431638](http://en.community.dell.com/techcenter/extras/m/white_papers/20431638)

- An iDRAC *Enterprise* license installed.

**Note:** For information iDRAC licensing, see the PowerEdge Software Licensing white paper located at: [http://en.community.dell.com/techcenter/extras/m/white\\_papers/20440637](http://en.community.dell.com/techcenter/extras/m/white_papers/20440637)



## 2 Configuring VNC Server on iDRAC

iDRAC exposed remote interfaces like GUI or Dell CLI client RACADM can be used to make required configuration settings.

iDRAC also has WSMAN command support, though it is more useful for programmable jobs. Relevant whitepapers for WSMAN commands can be referred from Dell Tech Center site and same logic can be applied to get/set VNC Server settings.

### 2.1 Using GUI

To configure VNC Server on iDRAC using GUI:


1. Connect to the iDRAC using a web browser.
2. Navigate to the *iDRAC Settings* -> *Network* page using the navigation pane.
3. Select the *Services* tab.
4. Jump to the *VNC Server* settings area using the link at the top of the page.



5. Check the *Enable VNC Server* check box.
6. Enter a strong password into the *VNC Password* and *Confirm Password* boxes.

**Note:** Anyone with this password and network connectivity to the iDRAC will be able to establish a remote desktop connection to this server.

7. Configure VNC session timeout as required, allowed range is 60-10800 seconds, default set is 300 seconds.
8. Configure VNC port to be used for connection, allowed range is 1024-65535. Standard and recommended port is 5901, which is set by default. Port configured here needs to be used by client to connect to this iDRAC VNC server.
9. Configure *SSL Encryption* value to enable/disable SSL encryption , to be used for connection between VNC Client on local machine and VNC Server on iDRAC.
  - a. To establish VNC connection without SSL, select 'Disabled'.


Integrated Dell Remote  
Access Controller 8

Navigate through Overview -> Network -> Services (tab) -> VNC Server

Support | About | Logout

System  
PowerEdge R330  
root , Admin

Overview  
Server  
Logs  
Power / Thermal  
Virtual Console  
Alerts  
Setup  
Troubleshooting  
Licenses  
Intrusion  
iDRAC Settings  
Network  
User Authentication  
Update and Rollback  
Server Profile  
Sessions  
Hardware  
Storage  
Host OS

Network | SSL | Serial | Serial Over LAN | **Services** | OS to iDRAC Pass-through

Services

Jump to: Local Configuration | Web Server | SSH | Telnet | Remote RACADM | SNMP Agent | Automated System Recovery Agent | **VNC Server**

SNMP Agent

Attribute	Value
Enabled	<input checked="" type="checkbox"/>
SNMP Community Name	public
SNMP Protocol	<input checked="" type="radio"/> All (SNMP v1/v2/v3) <input type="radio"/> SNMP v3
SNMP Discovery Port Number	161

Automated System Recovery Agent

Attribute	Value
Enabled	<input type="checkbox"/>

VNC Server

Attribute	Value
Enable VNC Server	<input checked="" type="checkbox"/>
VNC Password	••••••
Confirm Password	••••••
Max Sessions	1
Active Sessions	0
Timeout	300 seconds
VNC Port Number	5901
SSL Encryption	Disabled



- b. To establish VNC connection with SSL encryption i.e TLS/SSL tunneling set the *SSL Encryption* value to *Auto-Negotiate* or a specific cipher minimum strength (*128-bit or higher, 168-bit or higher, or 256-bit or higher*).

**Note:** Without TLS/SSL encryption data communicated in the remote desktop connection, including host credentials, may be exposed and the identity of the iDRAC cannot be verified. Consider disabling encryption only on secure local networks, or when protected by other security such as VPN encryption.

**Note:** Many VNC clients do not have integrated support for iDRAC compatible TLS/SSL tunneling. Use a compatible client or activate an external secure tunnel application such as '*stunnel*' prior to launching the VNC client.

10. Click *Apply* to enable the VNC server on iDRAC.

## 2.2 Using RACADM

To configure VNC Server on iDRAC using RACADM:

1. Establish ssh session with iDRAC using utility like puTTY.
2. Check existing VNC Server settings using command

```
/admin1-> racadm get idrac.vncserver
```

```
[Key=idrac.Embedded.1#VNCServer.1]
```

```
Enable=Disabled
```

```
!!Password=***** (Write-Only)
```

```
Port=5901
```

```
SSLEncryptionBitLength=Disabled
```

```
Timeout=300
```

3. To get possible values for any configuration of vnc server, like for "SSLEncryption", run following command

```
/admin1-> racadm help idrac.vncserver.SSLEncryptionBitLength
```

```
SSLEncryptionBitLength -- SSL Encryption Bit Length
```

```
Usage -- 0- Disabled 1- Auto Negotiate; 2- 128-Bit or Higher; 3- 168-Bit or Higher; 4- 256-Bit or Higher
```

```
Required License -- VNC Server
```

```
Dependency -- None
```





4. Enable VNC Server and configure required settings in following way.

```
/admin1-> racadm set idrac.vncserver.enable 1  
[Key=idrac.Embedded.1#VNCServer.1]  
Object value modified successfully  
/admin1-> racadm set idrac.vncserver.timeout 600  
[Key=idrac.Embedded.1#VNCServer.1]  
Object value modified successfully
```

With same approach, other attributes like port, password can be set.

5. To establish VNC connection WITHOUT SSL encryption, set encryption level to '0' ('disabled') using following command.

```
/admin1-> racadm set idrac.vncserver.SSLEncryptionBitLength 0  
[Key=idrac.Embedded.1#VNCServer.1]  
Object value modified successfully
```

6. Finally confirm if set values are reflecting

```
/admin1-> racadm get idrac.vncserver  
[Key=idrac.Embedded.1#VNCServer.1]  
Enable=Enabled  
!!Password=***** (Write-Only)  
Port=5901  
SSLEncryptionBitLength=Disabled  
Timeout=600
```

7. To establish VNC connection WITH SSL encryption, set required encryption level using following command.
  - a. To enable encryption i.e TLS/SSL tunneling set the *SSL Encryption* value to *Auto-Negotiate* or a specific cipher minimum strength, as seen in step 3 (*128-bit or higher, 168-bit or higher, or 256-bit or higher*).

```
/admin1-> racadm set idrac.vncserver.SSLEncryptionBitLength 1  
[Key=idrac.Embedded.1#VNCServer.1]  
Object value modified successfully  
/admin1-> racadm get idrac.vncserver  
[Key=idrac.Embedded.1#VNCServer.1]  
Enable=Enabled  
!!Password=***** (Write-Only)  
Port=5901  
SSLEncryptionBitLength=Auto Negotiate  
Timeout=600
```



**Note:** Without TLS/SSL encryption data communicated in the remote desktop connection, including host credentials, may be exposed and the identity of the iDRAC cannot be verified. Consider disabling encryption only on secure local networks, or when protected by other security such as VPN encryption.

**Note:** Many VNC clients do not have integrated support for iDRAC compatible TLS/SSL tunneling. Use a compatible client or activate an external secure tunnel application such as '*stunnel*' prior to launching the VNC client.



## 3 Establishing VNC connection using *RealVNC* VNC Client on Windows OS

**RealVNC** is a simple VNC viewer client package with integrated ability to establish VNC sessions with different encryption levels. This open-source software is available for free download from the project repository.

**Note:** RealVNC Viewer Client is also available for other OS like Linux, Solaris , Mac OS X. Also available as VNC viewer app on Android platform.

### 3.1 Installing RealVNC

To download and install RealVNC Viewer Client:

1. Download latest suitable(32-bit or 64-bit OS) vnc viewer client from realvnc website <https://www.realvnc.com/download/viewer/>
2. Install client as per instructions from website.

### 3.2 Connecting Using RealVNC without SSL

To establish VNC connection un-encrypted, both Client and Server side 'SSL encryption' needs to be disabled.

#### 3.2.1 Configuring iDRAC VNC Server for unencrypted VNC connection

1. To allow VNC connection without encryption , set the '*SSL Encryption*' value in iDRAC to '*Disabled*'.
2. As detailed in [section 2.1](#) step 9.a, GUI can be used to configure above 'SSL Encryption' value.
3. Or as detailed in [section 2.2](#) step 5, command line tool RACADM can be used to configure above 'SSL Encryption' value.

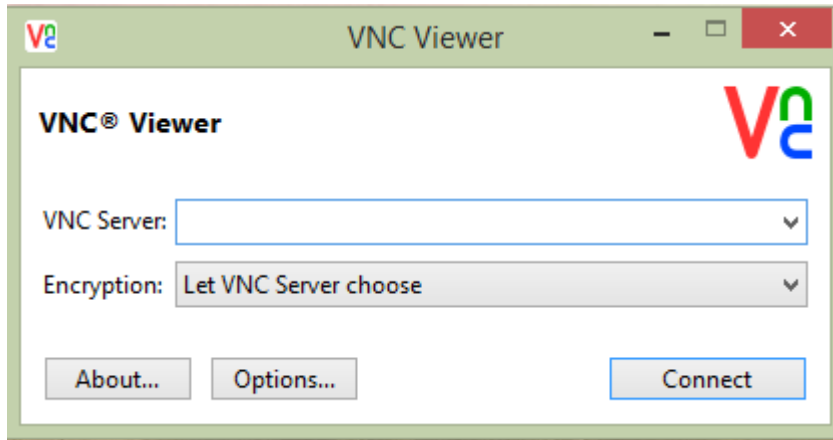
#### 3.2.2 Configuring RealVNC Client

To establish a VNC connection using RealVNC:

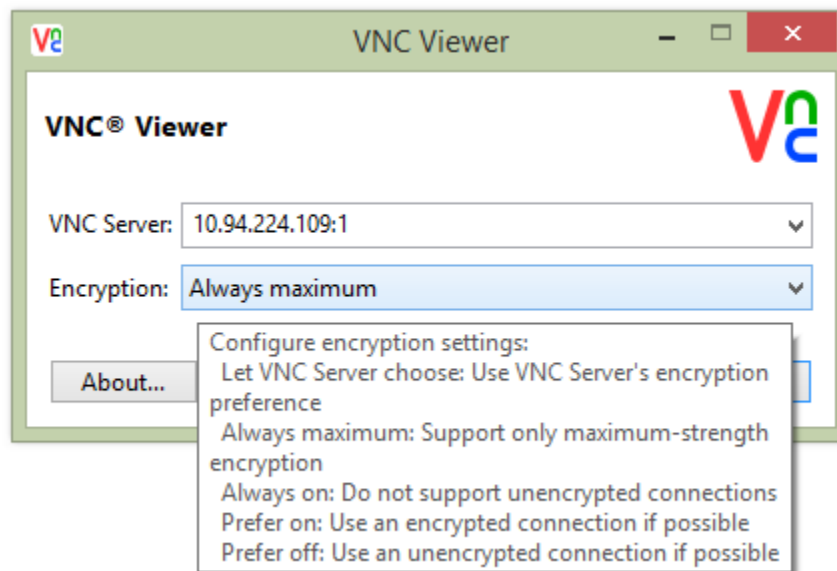
1. Launch the RealVNC Viewer Client application .
2. In the VNC Server :Display box enter the iDRAC IP address followed by the VNC port. For example: *10.94.224.109:5901* connects to the iDRAC at IP *10.94.224.109* on port *5901*.

**Note:** The default iDRAC VNC Port Number is 5901.

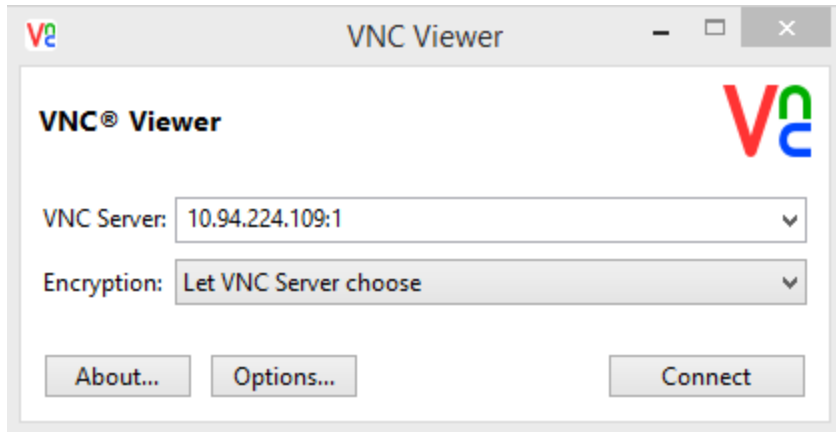




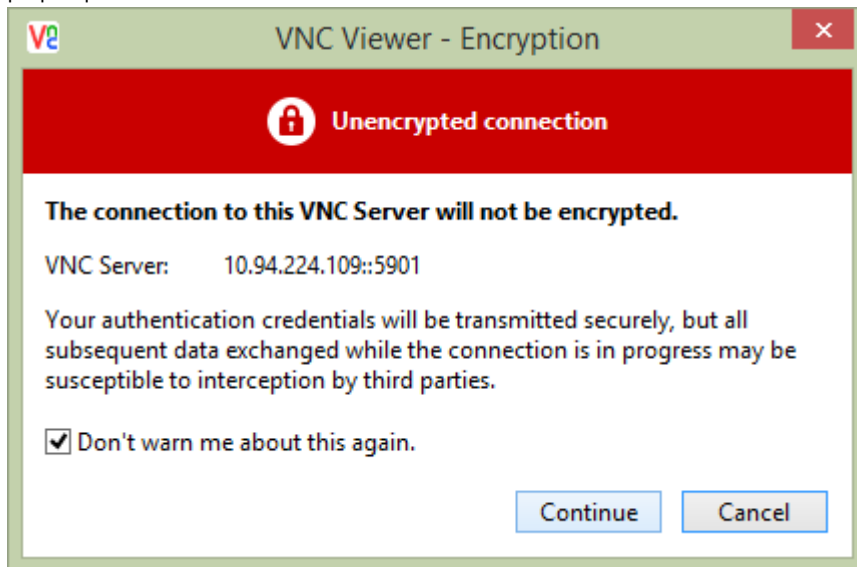
3. Available encryption levels in RealVNC Client are as depicted in screenshot below



For server to negotiate for best possible encryption, choose first option **“Let VNC Server choose”** for Encryption. This setting will work in both cases when SSL encryption is enabled or disabled on iDRAC VNC Server.



4. If *SSL Encryption* is disabled in the iDRAC *VNC Server* settings, following warning message may pop-up



5. Click *Continue* to begin establishing the VNC connection.
6. The VNC session to Server Host OS will be established, over unencrypted channel.

## 3.3 Connecting Using RealVNC over SSL, using ssltunnel

Like most VNC clients available today, RealVNC Viewer Client application is not having inbuilt capability to establish connection over SSL, an additional SSL Tunneling application needs to be used. One such application is 'ssltunnel', which creates and uses ssl tunnel for communication with server on other end, which is iDRAC VNC Server in this case.

'ssltunnel' needs to be configured to establish connection with iDRAC VNC Server. VNC client will connect to ssltunnel on loopback ip (127.0.0.1) and configured port(ex: 5930) and ssltunnel will in turn connect to configured ip of iDRAC VNC Server , **over SSL**.

### 3.3.1 Configuring iDRAC VNC Server for encrypted VNC connection

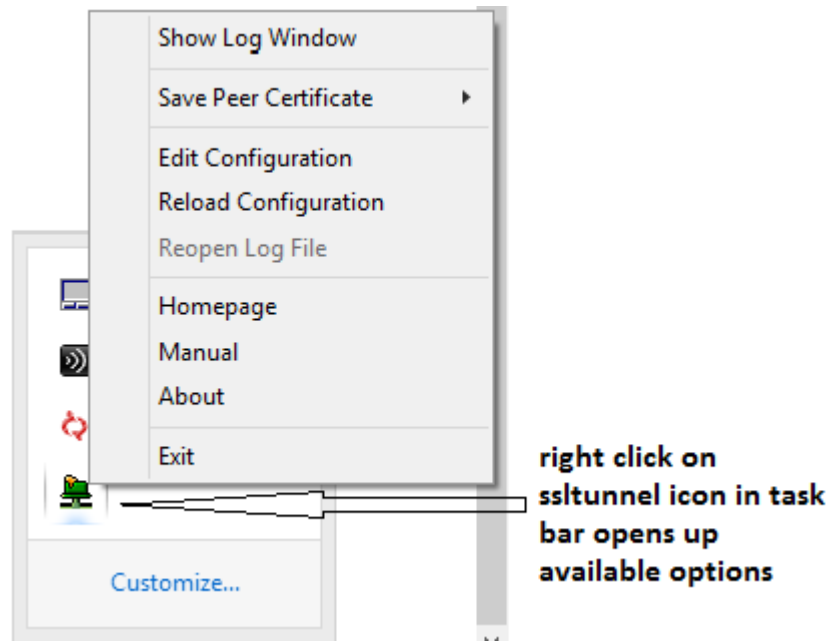
1. To allow VNC connection encryption i.e TLS/SSL tunneling set the '*SSL Encryption*' value in iDRAC to *Auto-Negotiate* or a specific cipher minimum strength i.e *128-bit or higher, 168-bit or higher, or 256-bit or higher*.
2. As detailed in [section 2.1](#) step 9.b, GUI can be used to configure above 'SSL Encryption' value.
3. Or as detailed in [section 2.2](#) step 7, command line tool RACADM can be used to configure above 'SSL Encryption' value.

### 3.3.2 Installing and configuring 'ssltunnel' application

1. '**ssltunnel**' currently available for download from <http://www.stunnel.org/downloads.html>
2. Install 'stunnel' and launch 'stunnel GUI start' from Program menu. Stunnel will start in background and can be located in Windows taskbar menu with following icon



3. Edit stunnel config.
  - a. Right click on stunnel icon and select 'Edit configuration', which will open stunnel.conf text file for editing.



- b. Add following config in sstunnel.conf file to allow ssltunnel connection to iDRAC VNC Server. After adding , save the file.

**[VNC-iDRAC]**

**client = yes**

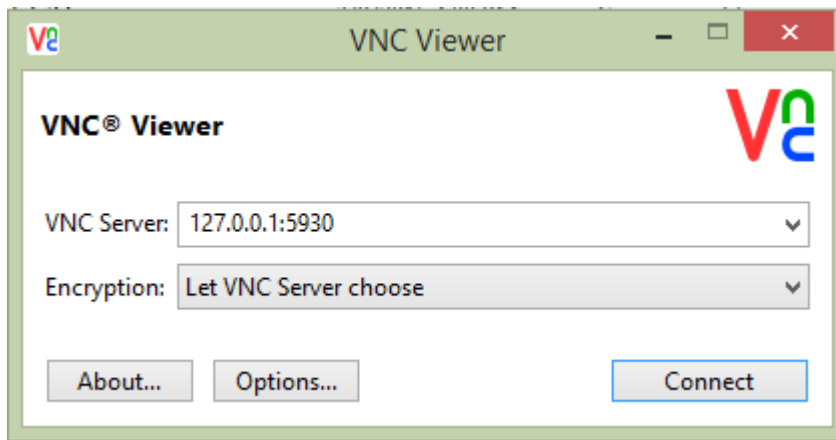
**accept = 127.0.0.1:5930**

**connect = 10.94.224.215:5901**

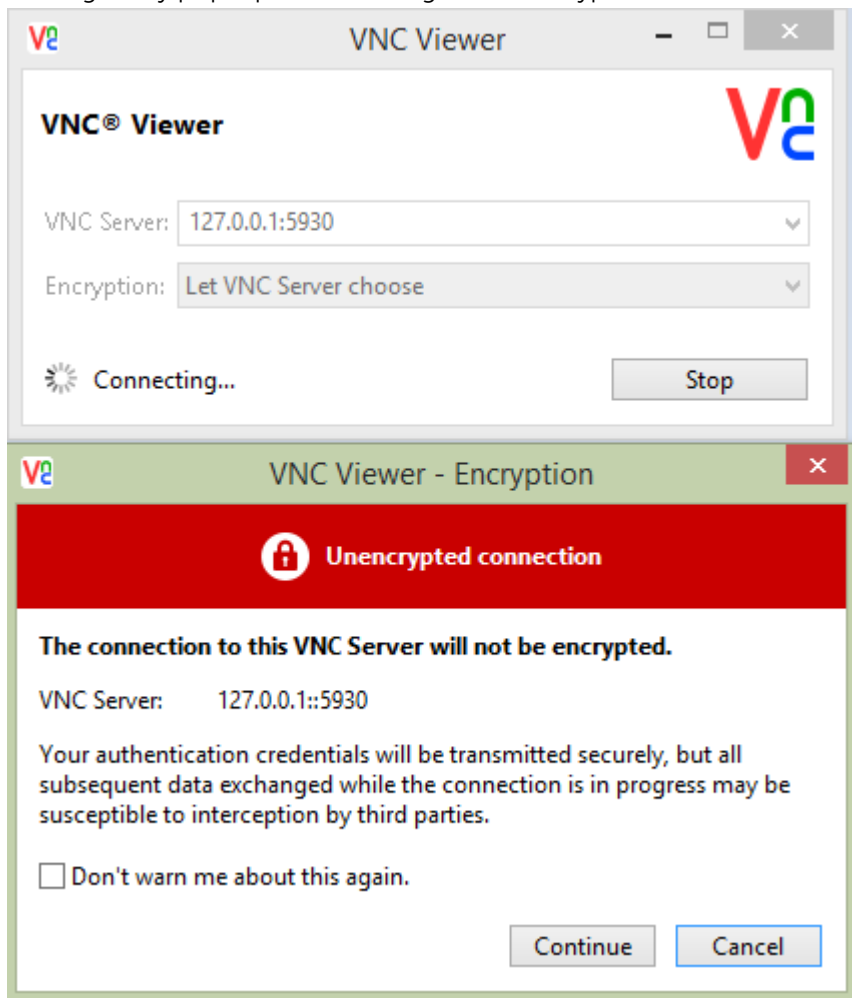
4. Reload modified stunnel config.
  - a. Right click on stunnel again from taskbar menu, click on 'Reload Configuration', which will make ssltunnel application to re-read the sstunnel.conf file and make new VNC Server related configuration into effect.
5. Now stunnel is ready to connect with iDRAC VNC server on configured port and listening for client connection on local loop back ip 127.0.0.1 , on port 5930.
6. So any connection request ssltunnel gets on local ip:port 127.0.0.1:5930 over an unencrypted channel, it will redirect the connection request to configured VNC Server ip:port here 10.94.224.215:5901, over ssl tunnel, making the connection encrypted and secure.

### 3.3.3 Configuring RealVNC Client to connect through SSL tunnel

1. Launch the RealVNC Viewer Client application .
2. Enter <ip address>:<port> configured in sstunnel where its listening for connection. As configured here, enter '127.0.0.1:5930'.
3. Select Encryption to 'Let VNC Server Choose' or value as configured in iDRAC .



4. Message may pop-up still , warning about unencrypted connection





Difference here is RealVNC client is trying connection with 'ssltunnel' application locally (on same machine) on an un-encrypted channel.

Ssltunnel in turn will in turn make encrypted connection over ssl tunnel to iDRAC VNC server, as desired.

5. Click 'Continue' in warning message pop-up window , to begin establishing the VNC connection over ssl.
6. The VNC session to Server Host OS will be established , encrypted over ssl tunnel .



## 4 Connecting securely with SSVNC Client on Windows

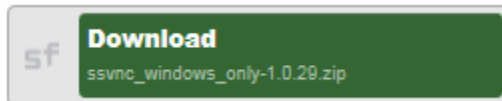
**SSVNC** is a VNC client package with integrated secure tunneling capabilities based on the Tight VNC viewer and STUNNEL program. It has been tested with the iDRAC with and without secure tunneling enabled. This open-source software is available for free download from the project repository.

**Note:** SSVNC is also available for Linux/Unix and Mac OS X.

### 4.1 Installing SSVNC

To download and install SSVNC:

7. Navigate to the ssvnc repository <http://sourceforge.net/projects/ssvnc/> in a web browser.
8. Download the latest preferred release (for example: *ssvnc\_windows\_only-1.0.29.zip*) using the provided link.

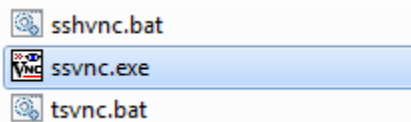


9. Extract the contents of the zip file.
10. The ssvnc Windows binary will be located under *<download-dir>/<archive-name>/ssvnc/Windows/ssvnc.exe* where *<download-dir>* is the download directory and *<archive-name>* is the name of the package (for example: *ssvnc\_windows\_only-1.0.29*, unless overridden by your zip extraction tool). You may wish to relocate the files and/or create a shortcut on the desktop, start menu, or quick launch bar.

### 4.2 Connecting Using SSVNC

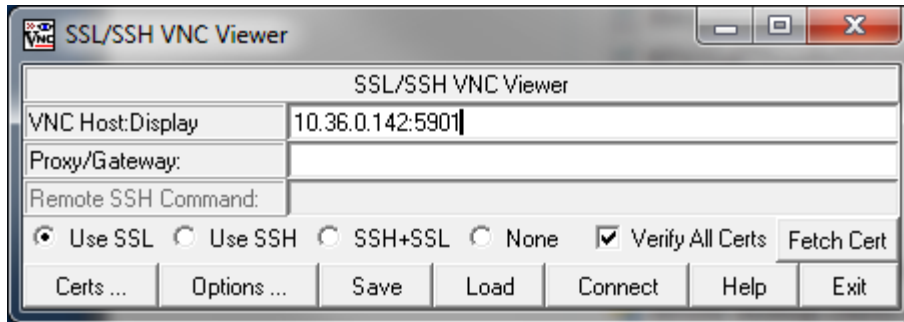
To establish a VNC connection using SSVNC:

11. Launch the SSVNC application by double clicking the *ssvnc.exe* file (or shortcut).



12. In the VNC Host:Display box enter the iDRAC IP address or hostname followed by the VNC port. For example: *10.36.0.142:5901* connects to the iDRAC at IP *10.36.0.142* on port *5901*.

**Note:** The default iDRAC VNC Port Number is 5901.



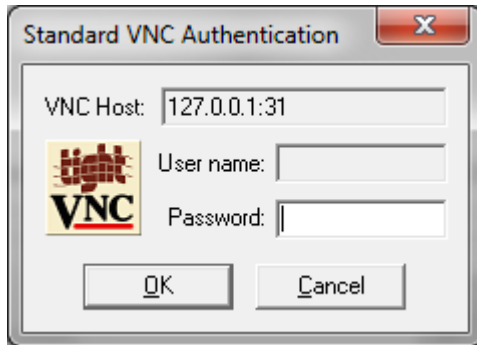
13. If *SSL Encryption* is enabled in the iDRAC *VNC Server* settings, ensure the *Use SSL* radio box is selected. Otherwise, *None* should be selected.
14. Click *Connect* to begin establishing the VNC connection.
15. If encryption is enabled, the certificate will be fetched.
  - a. In the *Unrecognized SSL Cert* dialog, Click *Inspect and maybe Save Cert...* to view the certificate information.
  - b. Verify the certificate information corresponds to the expected iDRAC SSL certificate. Once verified, click *Save* in the *Certificate* dialog.



**Note:** You can view the iDRAC SSL certificate in a web browser or iDRAC GUI. If the certificate information does not match, it may indicate a security issue and you should terminate the connection. For more information see the corresponding iDRAC User's Guide:  
<http://en.community.dell.com/techcenter/systems-management/w/wiki/3204.dell-remote-access-controller-drac-idrac>

- c. Click *Save* in the *Import/Save SSL Certificate* dialog to save the certificate and proceed.
- d. Click *OK* to acknowledge the certificate file was saved.
- e. Wait for the secure tunnel to be established.

16. When prompted in the *Standard VNC Authentication* dialog, enter the *VNC Password* from the iDRAC *VNC Server* settings and then click *OK*.



17. The VNC session will be established.

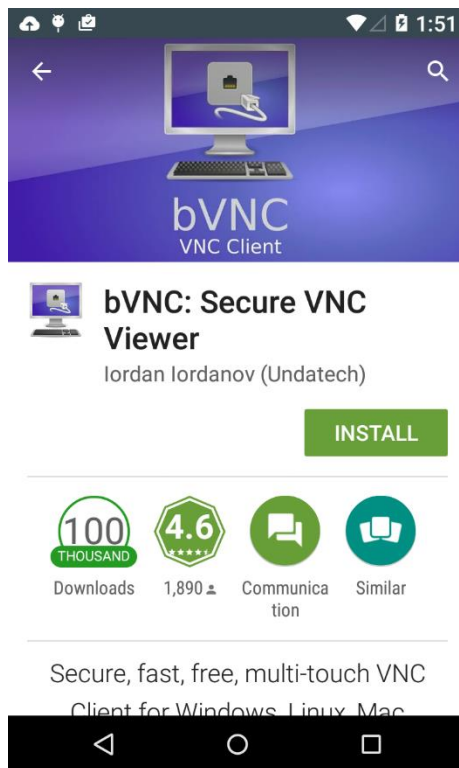
## 5 Connecting with bVNC Client on Android

While there are a number of VNC clients available for Android-based smartphones and tablets, not all VNC clients have integrated support for the iDRAC compatible secure tunneling functionality. The **bVNC** client has been tested with the iDRAC with and without secure tunneling enabled. Both free and donation-supported versions of the bVNC client are available from the Google Play Store.

### 5.1 Installing bVNC

To download and install bVNC from the play store:

1. Launch the Google *Play Store* app from the Android apps list or desktop.
2. In the search box, type *bVNC*.
3. Select bVNC: Secure VNC Viewer (free) or bVNC Pro: Secure VNC Viewer from the list.
4. Press the *Install* button.



**Note:** bVNC is also available in the Amazon Appstore, BlackBerry App World, and the GitHub source code repository.

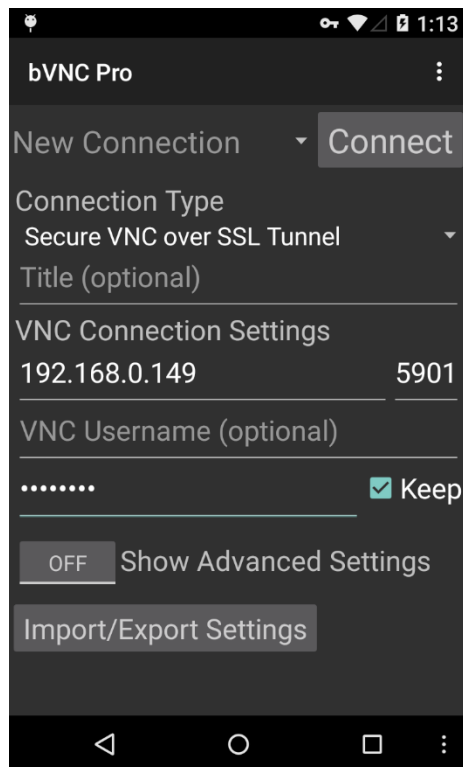
## 5.2 Connecting using bVNC

To configure and establish a connection using bVNC:

1. Launch *bVNC* from the Android apps list or desktop.
2. In the *Connection Type* box:
  - a. If *SSL Encryption* is enabled in the iDRAC *VNC Server* settings select *VNC over Secure Tunnel*.
  - b. Otherwise, select *Basic VNC*.
3. If desired, enter a connection name in the *Title* box. If blank, a name will be generated based on the host address and port number.
4. In the *VNC Server* box enter the iDRAC IP address or hostname.
5. In the *Port* box enter the *VNC Port Number* from the iDRAC *VNC Server* settings.

**Note:** The default iDRAC VNC Port Number is 5901. Most VNC applications, including bVNC default to 5900 and must be changed.

6. In the *VNC Password* box, enter the same password as entered in the iDRAC *VNC Server* settings.



7. Press *Connect* to begin establishing the VNC connection.
8. If encryption is enabled, the certificate verification dialog will appear. Verify the certificate information corresponds to the expected iDRAC SSL certificate. Once verified, click *Yes*.

**Note:** You can view the iDRAC SSL certificate in a web browser or iDRAC GUI. If the certificate information does not match, it may indicate a security issue and you should terminate the connection. For more information see the corresponding iDRAC User's Guide:

<http://en.community.dell.com/techcenter/systems-management/w/wiki/3204.dell-remote-access-controller-drac-idrac>

9. The VNC session will be established.

**Note:** Support for bVNC is integrated with Dell OpenManage Mobile (OMM). For more information on OMM see: <http://en.community.dell.com/techcenter/systems-management/w/wiki/4965.openmanage-mobile>





## 6 Accessing Virtual Media with VNC Session

Once VNC session is established using any of the client, including explained in previous sections, local media on a local system like desktop, laptop, can be mapped virtually to Server Host OS using Virtual Media feature in iDRAC. This feature is useful where quick data needs to be made available on Server Host OS remotely, like driver packages to update drivers on Host OS.

### 6.1 Launching Virtual Media

Launch can happen by navigating to Overview page->VirtualConsole section after login or from

Overview->Virtual Console page (highlighted in screenshot).

1. Click on 'Launch Virtual Console' link.
2. Pop-up message will ask to confirm redirection to Virtual Media, click on 'OK'.
3. In case of Internet Explorer Browser, Native activex plugin is used to launch Virtual Media screen or in case of any other Browser like Firefox, Java applet is used to launch.

The screenshot shows the Dell iDRAC Virtual Console interface. The 'Launch Virtual Console' link is highlighted in the 'Options' bar. A pop-up message asks for confirmation to continue using Virtual Media redirection. Below, the Virtual Console settings table is shown with various attributes like Enabled, Max Sessions, Active Sessions, Remote Presence Port, Video Encryption, Local Server Video, Plug-in Type, Default action upon session sharing request timeout, Automatic System Lock, and Keyboard/Mouse Attach State.

Attribute	Value
Enabled	<input type="checkbox"/>
Max Sessions	6
Active Sessions	0
Remote Presence Port	5900
Video Encryption Enabled	<input checked="" type="checkbox"/>
Local Server Video Enabled	<input checked="" type="checkbox"/>
Plug-in Type	Java
Default action upon session sharing request timeout	Full access
Automatic System Lock	<input checked="" type="checkbox"/>
Keyboard/Mouse Attach State	Auto-Attach

## 6.2 Mapping Virtual Media

Follow steps to below to map local media on to Server Host OS virtually

1. From Virtual Media redirected screen, click on "Virtual Media" tab.
2. Select required media mapping, either "Map CD/DVD" or "Map Removable disk".

The screenshot displays the Dell iDRAC Virtual Console interface. The top navigation bar includes the "System" tab, "PowerEdge R730", and "root, Admin". The left sidebar contains a navigation menu with options like Overview, Server, Logs, Power / Thermal, Virtual Console, Alerts, Setup, Troubleshooting, Licenses, Intrusion, iDRAC Settings, Hardware, Storage, and Host OS. The main area shows the "Virtual Console" window, which is currently displaying the "Virtual Media" tab. This tab contains a "Virtual Media" window with a "Transfer Rate" of 0 Kb/sec and a table for mapping media. The table has columns for "Target Drive", "Mapped To", "Read-Only", "Duration", and "Read/Write Bytes". The "Target Drive" column lists "CD/DVD" and "Removable Disk". The "Mapped To" column is empty. The "Read-Only" column has checkboxes. The "Duration" column is empty. The "Read/Write Bytes" column is empty. A "USB Reset" button is located at the bottom right of the "Virtual Media" window. Below the "Virtual Media" window, there is a "Virtual Console" section with various settings, including "Attribute", "Enabled", "Max Sessions", "Active Sessions", "Remote Presence Port", "Video Encryption Enabled", "Local Server Video Enabled", "Plug-in Type", "Default action upon session sharing request timeout", "Automatic System Lock", and "Keyboard/Mouse Attach State".

System  
PowerEdge R730  
root, Admin

Overview  
Server  
Logs  
Power / Thermal  
Virtual Console  
Alerts  
Setup  
Troubleshooting  
Licenses  
Intrusion  
iDRAC Settings  
Hardware  
Storage  
Host OS

Console

Options: > Launch Virtual Console

Since VNC session is active, Virtual Console is available.

Virtual Console

Attribute

Enabled

Max Sessions

Active Sessions

Remote Presence Port

Video Encryption Enabled

Local Server Video Enabled

Plug-in Type

Default action upon session sharing request timeout

Automatic System Lock

Keyboard/Mouse Attach State

Virtual Media

File Tools Virtual Media Help

Create Image ...

Map CD/DVD ...

Map Removable Disk ...

Transfer Rate: 0 Kb/sec

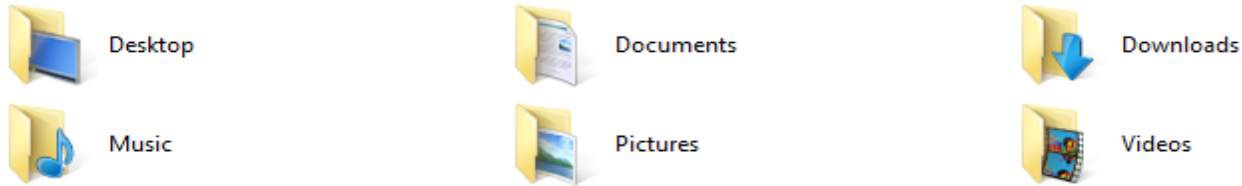
Target Drive	Mapped To	Read-Only	Duration	Read/Write Bytes
CD/DVD		<input type="checkbox"/>		
Removable Disk		<input type="checkbox"/>		

USB Reset

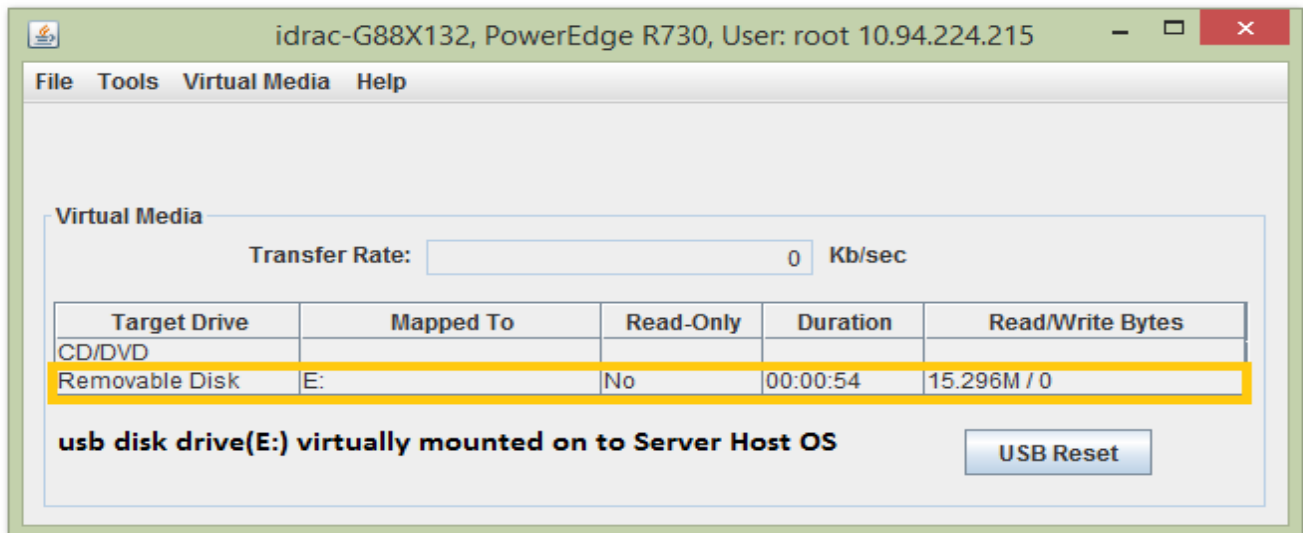
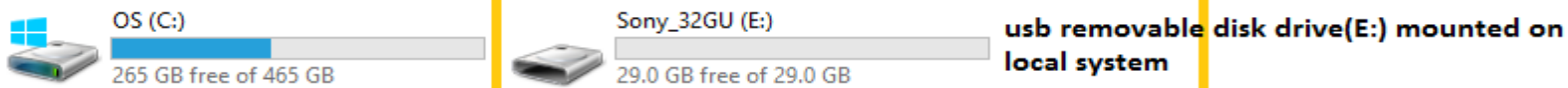
Apply

3. Example here shows mapping of removable disk , like any usb disk drive connected on local system.

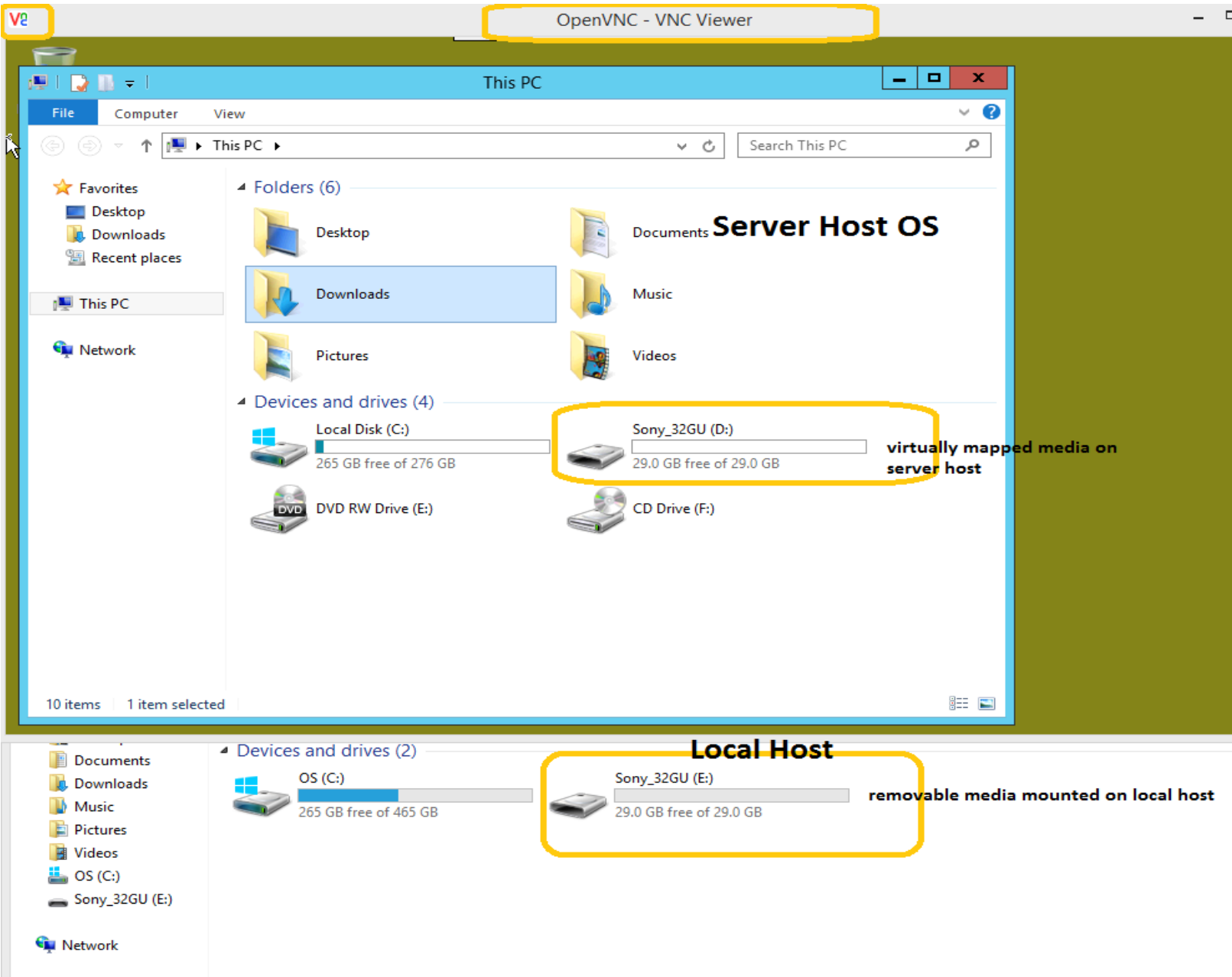
◀ Folders (6)



◀ Devices and drives (2)

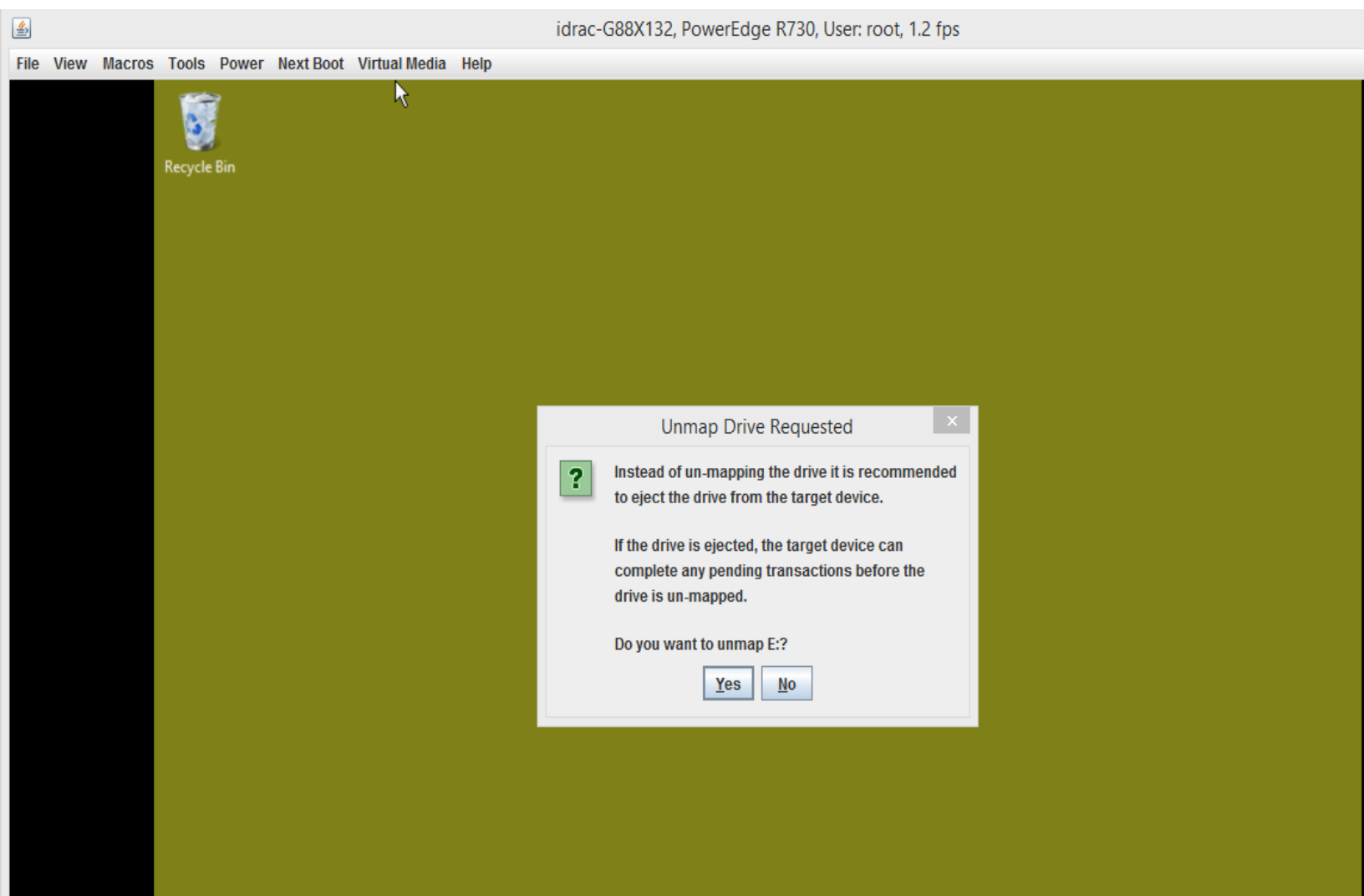


4. Same mapped media can be viewed and used on Server Host OS now.



## 6.3 UnMapping Virtual Media

1. After use, to unmap virtual media, click on same mapped device from Virtual Media tab, on Virtual Media screen. Pop-up screen 'Unmap Drive Requested' will appear to confirm.
2. However, instead of unmapping device its recommended to eject device from local system(desktop, laptop, etc) where it is originally connected.
3. Still if 'Unmap' needed just from Server Host OS alone, click 'Yes' on 'Unmap Drive Requested' pop-up screen.



## 7 Troubleshooting

The following procedures may assist in troubleshooting VNC connectivity.

1. **Symptom:** Unable to connect to iDRAC from VNC client
  - a. **Possible Cause:** Settings are incorrect  
**Resolution:** Verify the VNC server is enabled. Verify and/or adjust the remote host IP, port number, encryption settings, and password so the client and server values match.
  - b. **Possible Cause:** Network is unreachable  
**Resolution:** Verify network cables are attached or Wi-Fi connectivity is established. Verify required VPN connections are established. Verify network and firewall settings allow the iDRAC to be reached from the client. It may be useful to attempt to connect to the iDRAC GUI from the client device.
  - c. **Possible Cause:** VNC client does not support iDRAC encryption  
**Resolution:** Switch to a VNC client that supports secure tunneling, or use an external secure tunneling program like 'ssltunnel'. It may be useful to attempt to connect to the iDRAC with encryption disabled.
2. **Symptom:** Lost VNC connection to VNC server.
  - a. **Possible Cause:** VNC session timeout.  
**Resolution:** VNC session will remain active until session timeout period configured in iDRAC VNC server settings. Allowed session timeout period range is 60-10800 seconds
  - b. **Possible Cause:** Host system powercycled and If iDRAC NIC is in shared mode.  
**Resolution:** When iDRAC NIC is in shared mode and the host system is power cycled, the network connection is lost for few seconds. During this time, if you perform any action in the active VNC client, the VNC session may close. You must wait for timeout (value configured for the VNC Server settings in the Services page in iDRAC Web interface) and then re-establish the VNC connection.
  - c. **Possible Cause:** VNC Client window minimized for more than 60 seconds.  
**Resolution:** If the VNC client window is minimized for more than 60 seconds, the client window closes. You must open a new VNC session. If you maximize the VNC client window within 60 seconds, you can continue using it.
3. **Symptom:** VNC server shows active sessions when no clients are connected. Unable to connect to iDRAC from VNC client.
  - a. **Possible Cause:** VNC server state is invalid  
**Resolution:** Reset the iDRAC. Alternatively, disable and re-enable the VNC server from the iDRAC GUI. Consider reducing the VNC Server timeout value. Ensure the latest firmware is installed.

