Accessing Remote Desktop using VNC on Dell PowerEdge Servers and MX7000 Modular Infrastructure

This technical white paper provides information about establishing secure remote desktop connections to server host operating systems (OS) by using the standard VNC clients.

Abstract

Dell EMC PowerEdge servers support efficient and secure remote management tools. Virtual Network Computing (VNC) technology is incorporated in the iDRAC Enterprise firmware to support open and easy-to-use remote desktop functionality. This functionality is in addition to the browser-based remote console support accessible on the iDRAC GUI.

September 2018

Revisions

Date	Description
Sep 2018	Initial release

Acknowledgements

This paper was produced by the following members of the Dell EMC Server and Infrastructure Systems team:

Authors

Saurabh Kishore — Software Principal Engineer

Alex Rote — Software Senior Engineer

Contents

Executive summary

Dell EMC PowerEdge servers support efficient and secure remote management tools. Virtual Network Computing (VNC) technology is incorporated in the iDRAC Enterprise firmware to support open and easy-to-use remote desktop functionality. This functionality is in addition to the browser-based remote console support accessible on the iDRAC GUI.

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

This technical white paper describes how to enable VNC support on iDRAC and securely connect by using clients on Microsoft Windows, Android, and iOS platforms; these methods also generally apply to other platforms.

1 Introduction

Remote Desktop connections are useful in provisioning, monitoring, and troubleshooting systems. Similar to other remote desktop technologies, VNC servers and clients allow for a virtual keyboard, video, and mouse device (KVM) connection to the host OS. VNC clients are available for a variety of desktop and mobile platforms. This technical white paper explains how to establish a connection from VNC clients on the Microsoft Windows, Android, and iOS platforms—the procedures discussed are generic to other platforms.

The iDRAC VNC functionality is a complement to iDRAC Virtual Console functionality integrated with the Web GUI. VNC may offer greater usability, performance, or compatibility. For example, older versions of the Virtual Console required ActiveX or Java support that may be unavailable in some environments and mobile clients benefit from a customized mobile user interface (UI). Based on your system, there may be limitations on the simultaneous use of or number of Virtual Console and/or VNC sessions.

For security, it is recommended that the connection be encrypted with compatible SSH or TLS/SSL tunnels. With the 14th generation servers, support for VNC over SSH allows VNC to be used with iDRAC credentials, which in turn may be integrated with an LDAP directory server that enforces strong password policies. VNC over SSH clients are available for major platforms including iOS. On 12th and 13th generation PowerEdge servers, a dedicated VNC password is used and may be encrypted by using a TLS tunnel on Windows and Android.

From a mobile device, OpenManage Mobile (OMM) may be used to configure and start a remote console session when a compatible VNC client is installed. On the 14th generation servers equipped with Quick Sync 2, the OMM enables remote console support over the Quick Sync 2 Wi-Fi interface.

The Virtual Media feature is available by using both the Virtual Console and VNC sessions. If a VNC session is active, you can launch only the Virtual Media by using Launch Virtual Console and not the Virtual Console Viewer, as explained in Section 6 of this technical white paper.

1.1 System requirements

The iDRAC VNC is available on the following servers:

- 14th generation servers (with iDRAC 9). A 14G server is required for VNC over SSH support
- 13th generation servers (iDRAC8)
- 12th generation servers (iDRAC7) with firmware version 1.50.50 or later.

Note: For information about applying iDRAC7 firmware updates, see the white paper located at: http://en.community.dell.com/techcenter/extras/m/white_papers/20431638

Also, an iDRAC Enterprise license must be installed. Trial licenses may be available.

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

2 Configuring the iDRAC VNC server

The iDRAC VNC server is disabled by default and must be configured to be used. There are a number of general- and security-related settings.

The iDRAC VNC settings may be configured by using the web GUI or RACADM Command Line Interface

(CLI) as described in this document. Settings may also be changed by using programmatic interfaces such as WS-Man. For more information about WS-Man, see the Dell Tech Center resources provided in Technical support and resources.

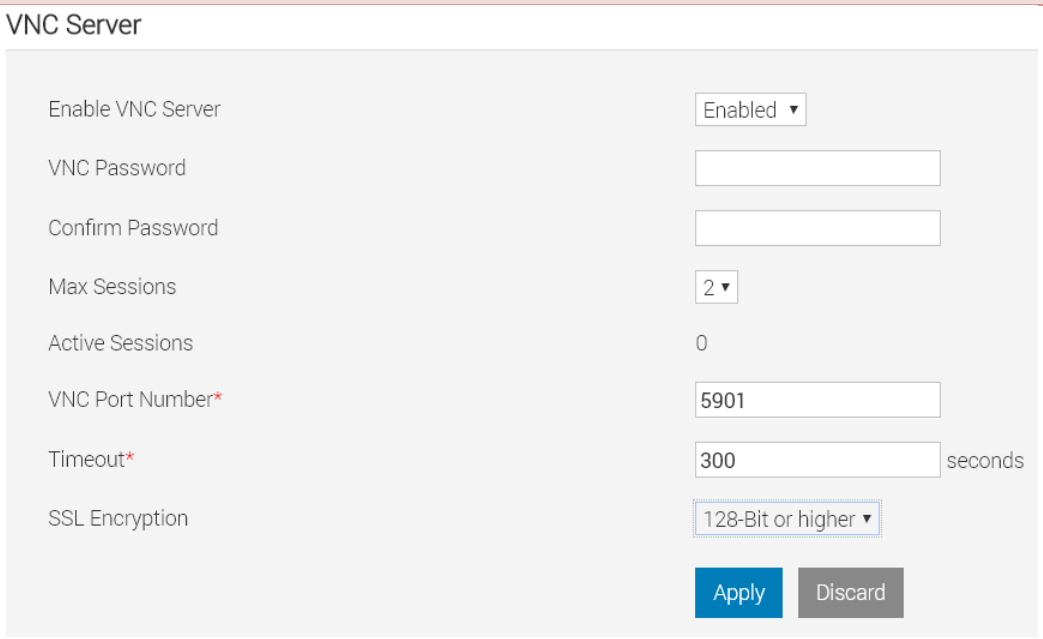
2.2 General VNC server settings

The VNC server attributes are:

Attribute	Description
Enable VNC Server	Enable the server to use VNC. By default, the VNC server is disabled.
Max Sessions	The maximum number of sessions to allow. On a 14G system, up to two sessions are supported, on a 13G or 12G server only one session is supported. Additional sessions consume more resources.
Active Sessions	This reflects the number of sessions in use, the maximum number of sessions cannot be exceeded. If this appears to be in error, the VNC server may need to be reset, see Troubleshooting issues when accessing remote desktop using VNC.
Timeout	The session timeout ranges from 60–10800 seconds (3 hours). The default is 300 seconds (5 min).
Port Number	The TCP Port number to use. By default, this is 5901. **Note**—Many VNC clients default to port 5900. However, by default, iDRAC uses port 5900 for the web Virtual Console. If using the iDRAC default properties, be sure to set the port number on the client to 5901.

2.3 Security-Related VNC server settings

The iDRAC VNC server supports three major operating modes:

Mode	Description
VNC over SSH	Dell 14G servers support VNC over SSH. This mode is automatically enabled if both VNC and SSH are enabled; SSH is enabled by default. To use VNC over SSH, authenticate to SSH with iDRAC credentials (username/password). **Note**—VNC over SSH is not compatible with VNC over TLS. When using VNC over SSH, set the SSL Encryption setting to disabled. To enable VNC over SSH only, do not set a VNC password. **Note**—To use VNC over SSH using only iDRAC credentials, enter the iDRAC wired IP address as the remote destination IP of the SSH tunnel (rather than localhost or the Quick Sync 2 IP). This requires the wired interface have an IP assigned. Otherwise, you must set and enter a VNC password. Some clients use localhost when establishing a tunnel automatically, and thus require a VNC password.
VNC over TLS	VNC over TLS (SSL) provides an encrypted connection on 14G/13G/12G servers. This mode is configured in the VNC settings and requires a VNC password.  Figure 1 VNC encryption is enabled
No Encryption	Using VNC without encryption offers greater compatibility and may be useful when troubleshooting remote desktop connectivity. In this mode, connections are still authenticated with a shared VNC password. **Note**—Without SSH or 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.

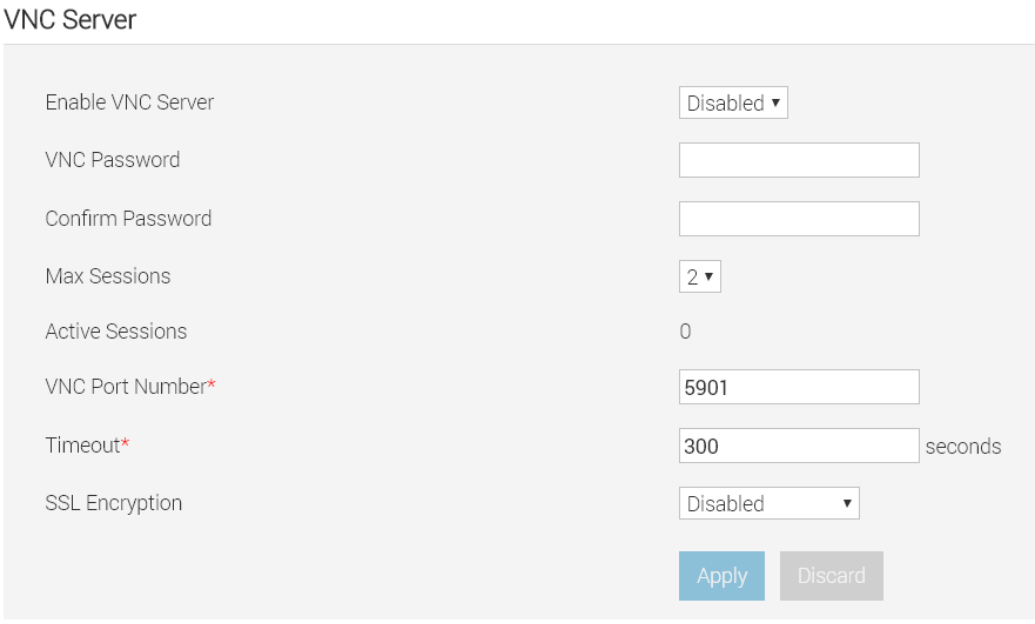


Figure 2 VNC encryption is disabled

The VNC security attributes are as follows:

Attribute	Description
VNC Password	Use this to set a VNC password. This password is used only by VNC. It is shared among all VNC connections and is not associated with a username.
	Note—Anyone with this password and network connectivity to the iDRAC will be able to establish a remote desktop connection to this server.
Confirm Password	When setting a VNC password, reenter the password here to verify it was entered correctly.
SSL Encryption	This constrains the TLS/SSL symmetric encryption key bit length. This may be set to *Disabled*, *Auto-Negotiate*, *128-bit or higher*, *168-bit or higher*, or *256-bit or higher*.

2.4 Configuring VNC by using the iDRAC GUI

To configure VNC settings by using the iDRAC GUI:

1. Connect to the iDRAC by using a web browser
2. Navigate to the iDRAC VNC settings

    a. On a 14G server (or blade), click **Configuration → Virtual Console** and scroll down to the VNC section. See Figure 1.

    b. On a 13G or 12G server, click **iDRAC Settings → Network** in the navigation page, click the **Services** tab, and then go to the **VNC Server** settings by using the link at the top of the page. See Figure 2.

3. Enable the VNC server by using the drop-down menu or check box.
4. Configure the VNC settings as necessary by using the drop-down menu or text boxes as appropriate.
5. Click **Apply** to activate configuration changes and enable the VNC server.

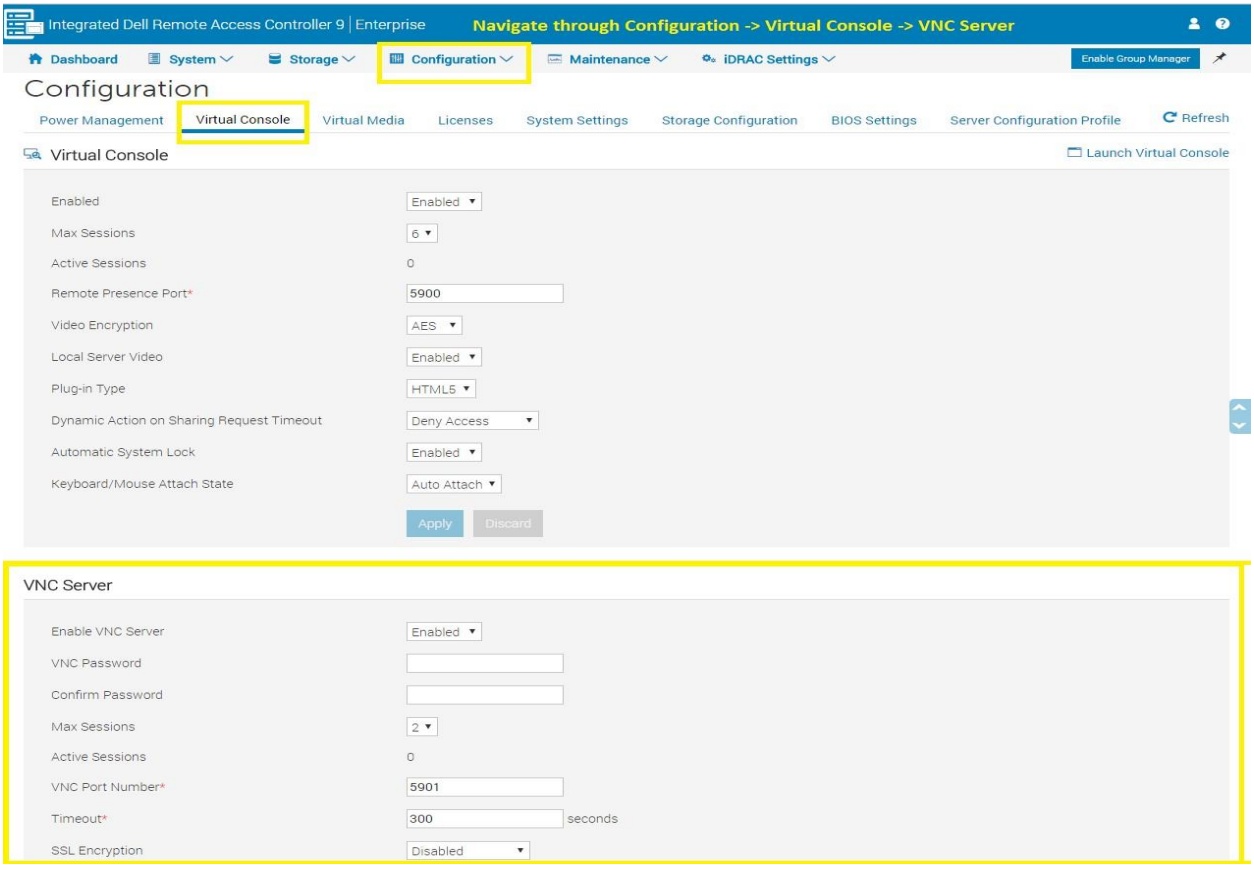


Figure 3 Configure VNC by using iDRAC GUI

Note—To enable or disable SSH to support VNC over SSH on 14G systems, click **iDRAC Settings → Services → SSH**.

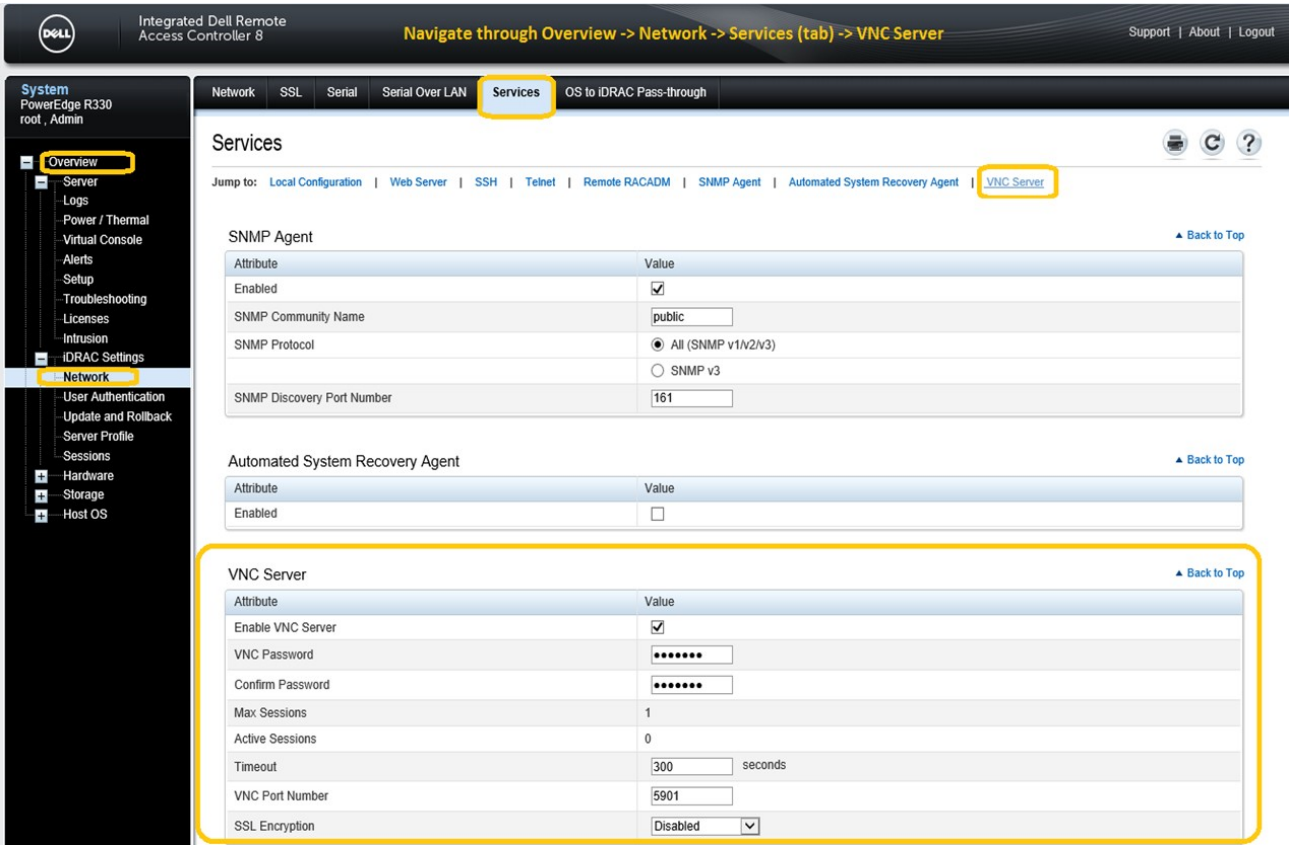


Figure 2 The 13G or 12G iDRAC GUI VNC settings

2.5 Configuring VNC by using RACADM CLI

1. Start a RACADM session by using the Dell Remote RACADM client or an SSH client such as PuTTY.
2. Check the existing VNC Server settings:

```
/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 a configuration option, run the `help` 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 the VNC Server and configure necessary settings:

```
/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
```

5. Ensure that the values are set correctly:

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

3 Connecting Windows with SSVNC Integrated Tunneling

SSVNC is a VNC client that includes integrated support for VNC over SSH and VNC over TLS encryption protocols, allowing it to connect to iDRAC securely without configuring multiple applications. 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.

3.1 Installing SSVNC

To download and install SSVNC:

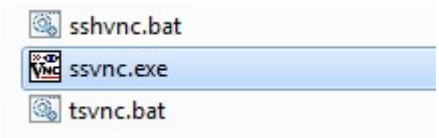
1. Navigate to the ssvnc repository http://sourceforge.net/projects/ssvnc/ in a web browser.
2. Download the latest preferred release (for example: ssvnc_windows_only-1.0.29.zip) using the provided link.

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

3.2 Connecting by using SSVNC

Prior to starting a connection, iDRAC must be configured as described in Configuring the iDRAC VNC server. To establish a VNC connection by using SSVNC:

1. Start the SSVNC application by double-clicking the ssvnc.exe file (or shortcut).



2. In the **VNC Host:Display** box, type 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`. If using VNC over SSH, type the iDRAC username to use. For example, `root@10.35.0.78:5901`.

Note—The default iDRAC VNC Port Number is 5901. If using VNC over SSH with SSVNC, you must configure a VNC password on iDRAC.

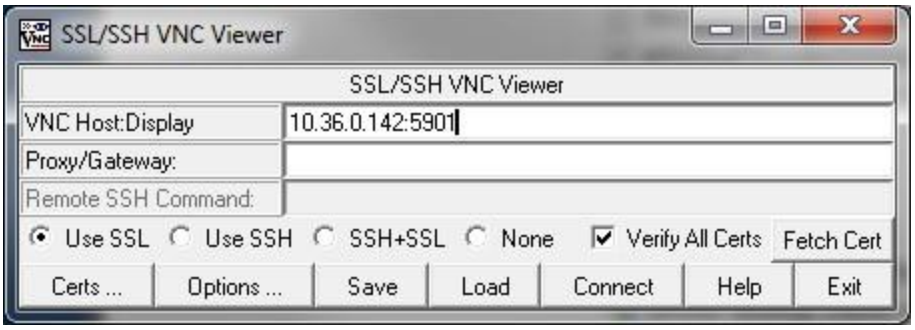


Figure 4 Connecting VNC by using SSVNC

3. The radio button selection should match the iDRAC configuration. To use VNC over SSH, select **Use SSH**.
4. Else, if SSL Encryption is enabled in the iDRAC VNC Server settings, ensure that **Use SSL** is selected. Else, **None** must be selected.
5. Click **Connect** to start the VNC connection.
6. If SSH is used, you may be prompted to accept the server's SSH key and you will be prompted to enter the iDRAC password associated with the SSH username. If TLS/SSL encryption is enabled, the certificate will be fetched.

    a. In the **Unrecognized SSL Cert** dialog box, click **Inspect and maybe Save Cert** to view the certificate information.
    b. Ensure that the certificate information corresponds to the expected iDRAC SSL certificate. After verification, click **Save** in the **Certificate** dialog box.

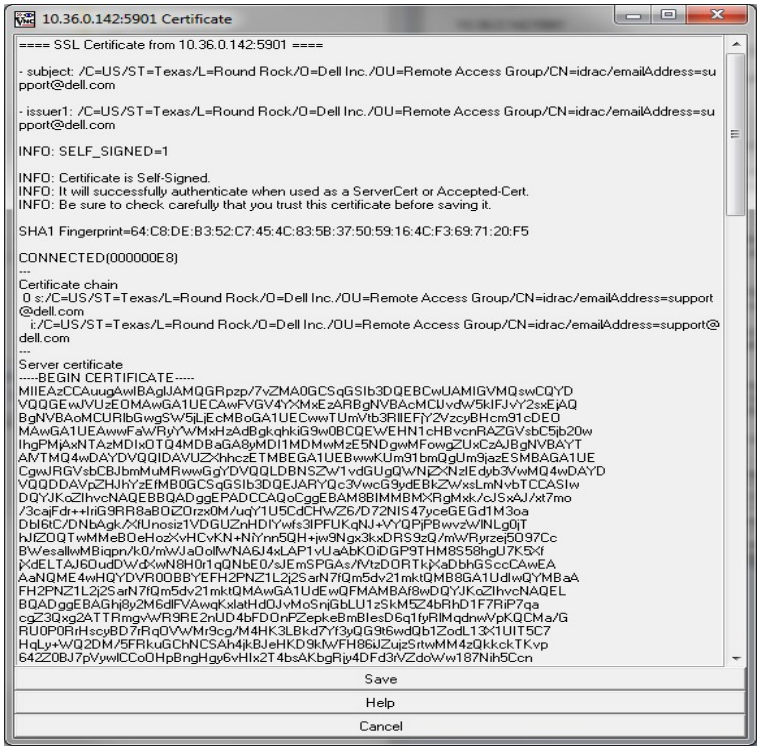


Figure 5 iDRAC SSL certificate

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 box to save the certificate and continue.
d. Click **OK** to acknowledge the certificate file was saved.
e. Wait for the secure tunnel to be established.

7. When prompted in the **Standard VNC Authentication** dialog box, type the *VNC* password from the ***iDRAC VNC Server*** settings, and then click **OK**.

   The VNC session is started.

Figure 6 Standard VNC authentication

4 Connecting Windows with RealVNC and external tunnels

RealVNC is a simple VNC viewer client package. Because RealVNC does not support standards-based encryption protocols, it may be used in unencrypted mode, or with external TLS or SSH tunnel clients. Therefore, the general procedures used to start an external tunnel may be used with other clients.

Note—The RealVNC clients are also available for other OSs such as Linux, Solaris, Mac OS X, Android, and iOS. For more information about using RealVNC on iOS, see Connecting iOS with RealVNC Viewer, Remoter Pro, and Remotix.

4.1 Installing RealVNC

To download and install RealVNC Viewer Client:

1. Download the latest suitable (32-bit or 64-bit) VNC viewer client from the RealVNC website https://www.realvnc.com/download/viewer/.
2. Install client as per instructions shown on the website.

4.2 Connecting by using RealVNC without encryption

To start an unencrypted VNC connection, both Client and Server side encryption settings must be disabled. To disable encryption on the iDRAC, set the '*SSL Encryption'* value in iDRAC to '*Disabled'*, and be sure to set a VNC password. For more information about configuring iDRAC VNC settings by using the GUI, see Configuring VNC by using the iDRAC GUI. For more information on configuring settings using the RACADM command line, see Configuring VNC by using RACADM CLI.

To establish a VNC connection by using RealVNC:

1. Start the RealVNC Viewer Client application.
2. In the **VNC Server address** box, type the iDRAC IP address followed by the VNC port. For example, `198.51.100.215:5901` connects to the iDRAC at IP 198.51.100.215 on port 5901. Press enter or click the highlighted connection action to connect.

Note—The default iDRAC VNC port number is 5901.

Figure 7 VNC viewer

3. Because the connection is not secure, the following message is displayed:

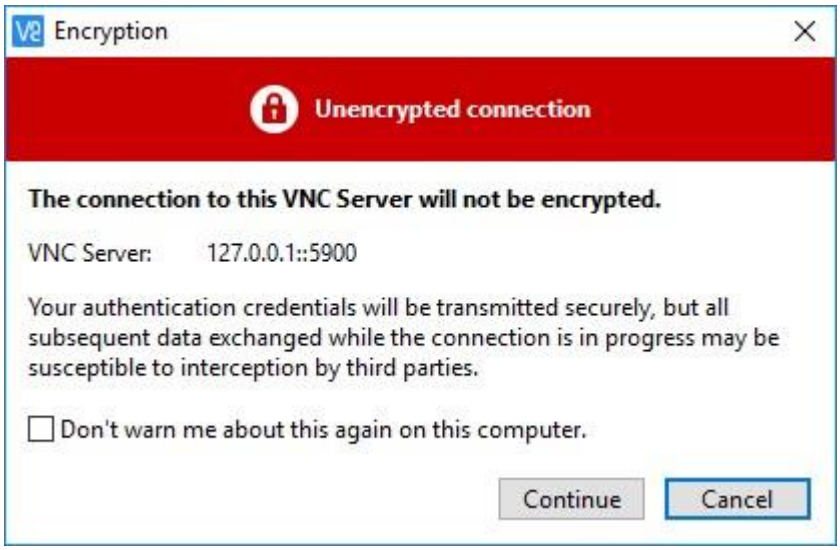


Figure 8 Unencrypted connection to the VNC server

4. Click **Continue** to begin establishing the VNC connection.
5. When prompted, type the VNC password.
6. The VNC session to Server Host OS will be started by using an unencrypted channel.

4.3 Connecting Using RealVNC over TLS/SSL by using ssltunnel

The TLS/SSL encryption provides protection against information disclosure on the 12G, 13G, and 14G servers. Similar to many VNC clients, RealVNC does not have built-in TLS support. However, a secure connection can be achieved by using RealVNC with an external tunneling application. One such application is ‘ssltunnel’. By first configuring ‘ssltunnel’ to establish a connection with the iDRAC VNC Server, the VNC client will connect to a local socket on the client system which will then securely forward data to the server.

To enable TLS/SSL encryption on the iDRAC, set the '*SSL Encryption'* value in iDRAC to **Auto-Negotiate**, or a specific minimum key length, *128-bit or higher*, *168-bit or higher*, or *256-bit or higher*. For more information about configuring iDRAC VNC settings by using the GUI, see Configuring VNC by using the iDRAC GUI. For more information on configuring settings using the RACADM command line, see Configuring VNC by using RACADM CLI.

4.3.1 Installing and configuring the 'ssltunnel' application

To use ssltunnel:

1. Download '**ssltunnel**' from http://www.stunnel.org/downloads.html.
2. Install 'stunnel' and start 'stunnel GUI start' from the Program menu. Stunnel will start in background and can be located in Windows taskbar with the following icon:

3. Edit the stunnel configuration:
   a. Right-click **stunnel** and select **Edit Configuration**. This will open the **stunnel.conf** text file for editing.

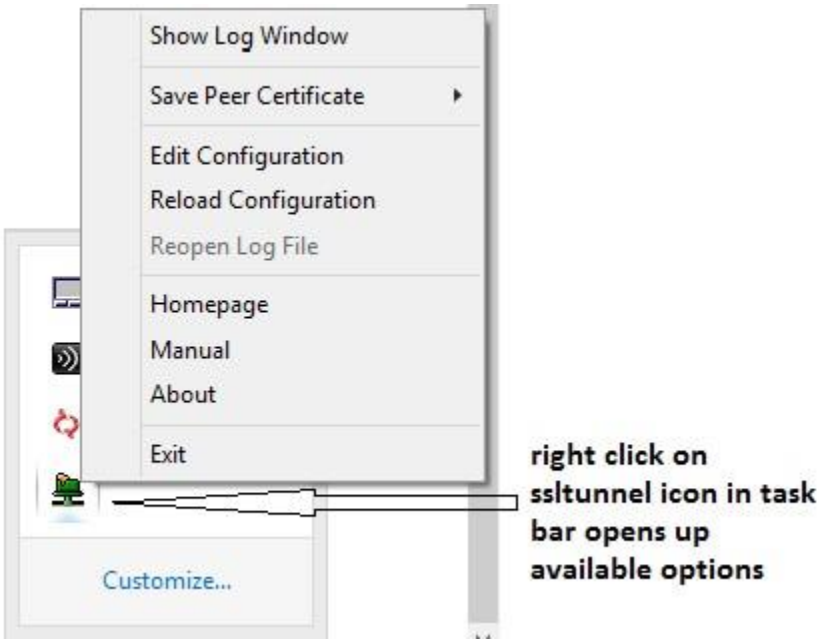


Figure 9 Edit stunnel configuration

   b. Add a configuration entry in the stunnel.conf file for the connection to the iDRAC VNC Server similar to the following example and save the file. In the lines below, substitute the iDRAC IP and VNC port in place of 198.51.100.215:5901*I,* and an available local port in place of 5930.

```
[VNC-iDRAC] client = yes
accept = 127.0.0.1:5930
connect =
198.51.100.215:5901
```

4. Load the modified stunnel configuration. Right-click the stunnel taskbar icon, and then click **Reload Configuration**. The updated configuration will take effect.
5. Connections to the local stunnel port will now be encrypted and forwarded to the iDRAC.

4.3.2 Using RealVNC Client with a local TLS/SSL tunnel

To use RealVNC with a local TLS/SSL tunnel:

1. Start the RealVNC Viewer Client application.
2. Connect the client to the local tunnel port by entering the local address as the server address. For example, '127.0.0.1:5900'. Because the VNC client is unaware of the encryption, leave the encryption level (within preferences) set to a value that does not require encryption such as 'let VNC Server choose'.

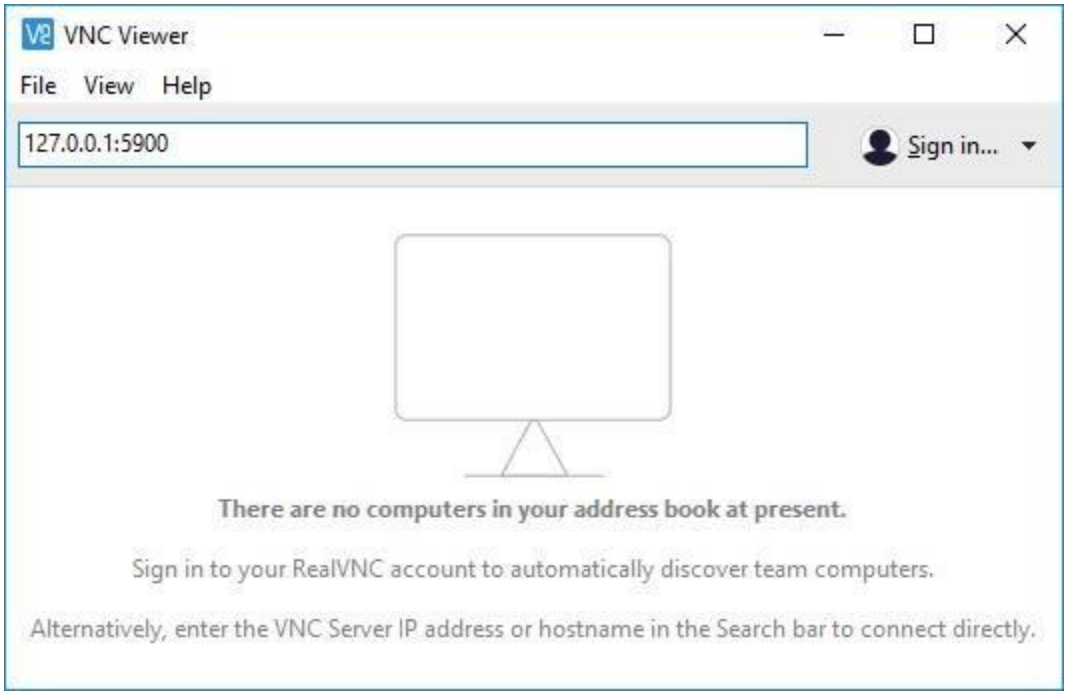


Figure 10 Use ReaVNC Client with a local TLS/SSL tunnel

3. Press Enter or select the list item to connect.
4. Because the client is unaware of the encryption, it may show an inaccurate warning indicating that the connection is unencrypted. Click continue to complete the connection.
5. When prompted, type the VNC password.
6. The VNC session to Server Host OS will be started over an encrypted channel.

4.4 Connecting using RealVNC over SSH

SSH tunneling provides protection against information disclosure on the 14G PowerEdge servers. The SSH connection is established by using iDRAC credentials, and need not require a separate VNC password. Similar to many VNC clients, RealVNC does not have built-in SSH support. However, a secure connection can be achieved by using RealVNC with an external SSH application's tunneling capabilities. One such

application is ‘PuTTY. By first configuring ‘PuTTY' to establish a connection with iDRAC SSH Server, the VNC client will connect to a local socket on the client system which will then securely forward data to the server.

Because the SSH tunneling is not compatible with TLS/SSL encryption, set the ‘*SSL Encryption’* value in iDRAC to *Disabled*. The iDRAC SSH server and VNC server must remain enabled. For more information about configuring iDRAC VNC settings by using the GUI, see Configuring VNC by using the iDRAC GUI. For more information on configuring settings using the RACADM command line, see Configuring VNC by using RACADM CLI.

4.4.1 Installing and configuring PuTTY

1. Download, install, and start PuTTY. It can be downloaded from: https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html
2. Configure PuTTY.
   a. Under **Connection → SSH →Tunnels**, add a tunnel. In the **Source Port** box, specify a local available port. For example, `5900`.
   b. In the **Destination** box, type IP address of the iDRAC wired interface followed by the VNC port. For example `198.51.100.215:5901`.

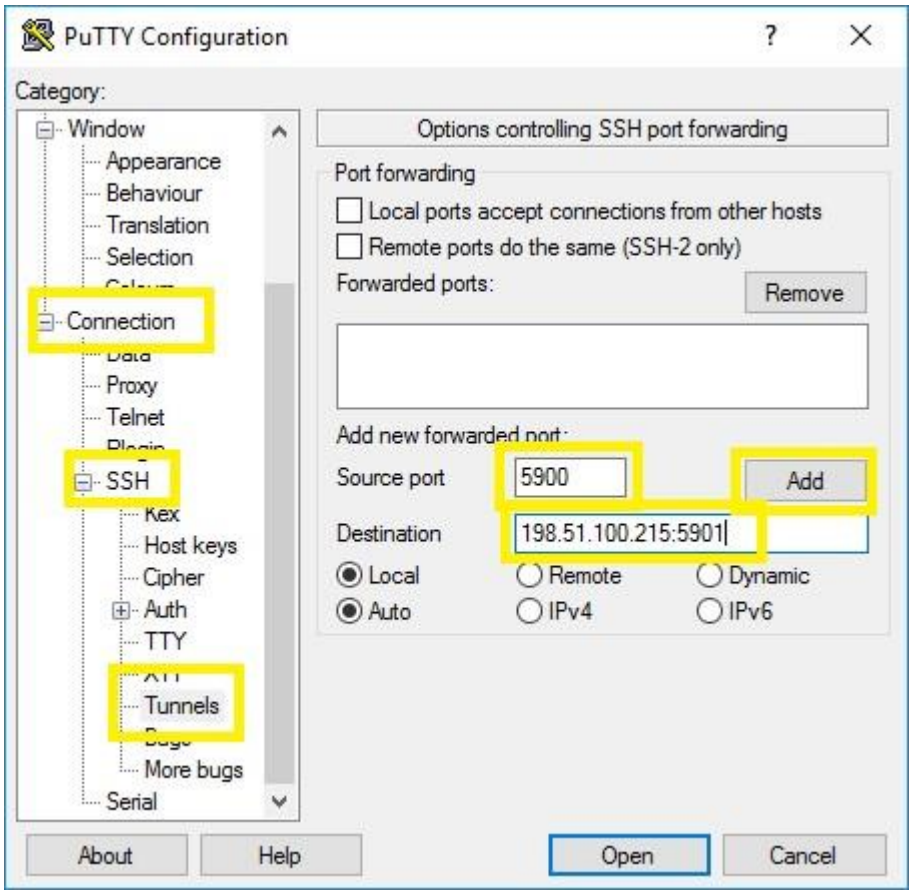


Figure 11 Configuring PuTTY

The connection will appear in the forwarded ports list:

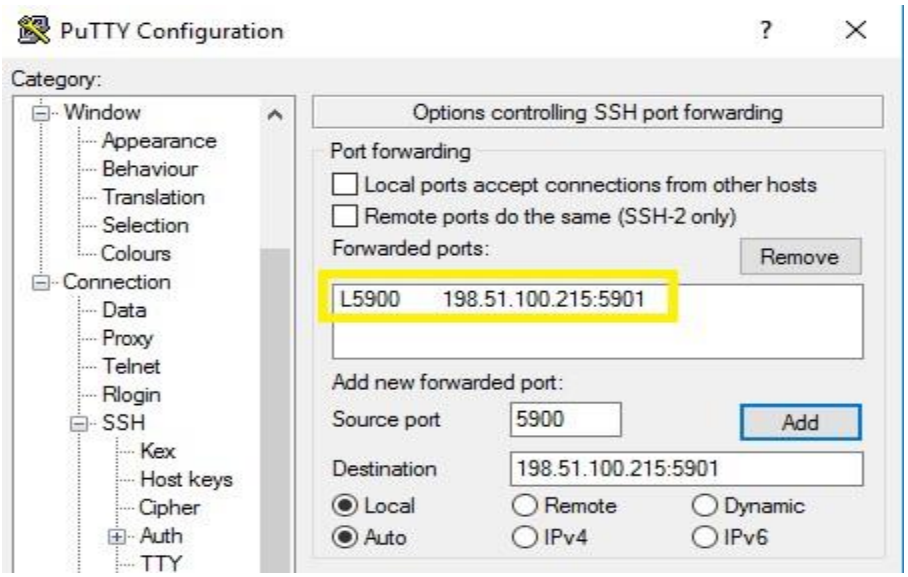


Figure 12 PuTTY configuration—Options controlling SSH port forwarding

c. Return to the **Session** page and type IP address of the iDRAC.
d. To save the session for a later reuse, type a name in the **Saved Sessions** box and click **Save**.

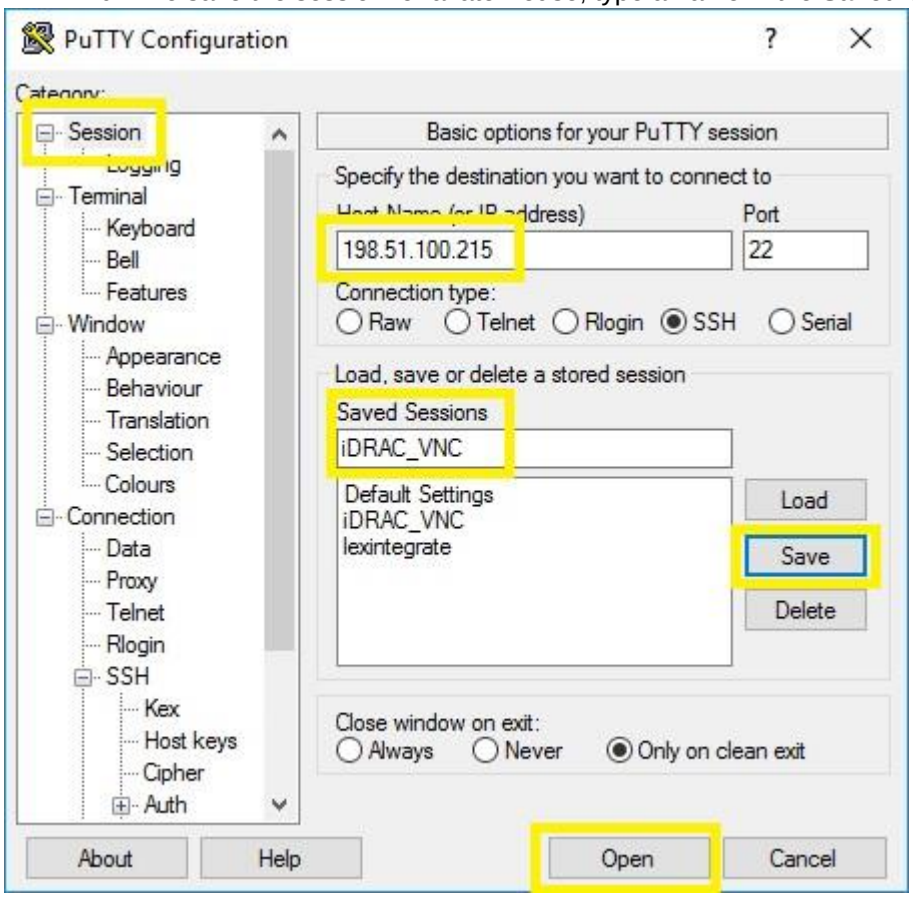


Figure 13 PuTTY configuration—Basic options for your PuTTY session

3. Click **Open** to connect to iDRAC and establish the tunnel.
4. Click **Yes** to accept the remote server Key.
5. Enter your iDRAC credentials when prompted.
   An SSH tunnel is now established.

4.4.2 Using RealVNC Client with a local SSH tunnel

1. Start the RealVNC Viewer Client application.
2. Connect the client to the local tunnel port by typing the local address as the server address. For example, `127.0.0.1:5900`.

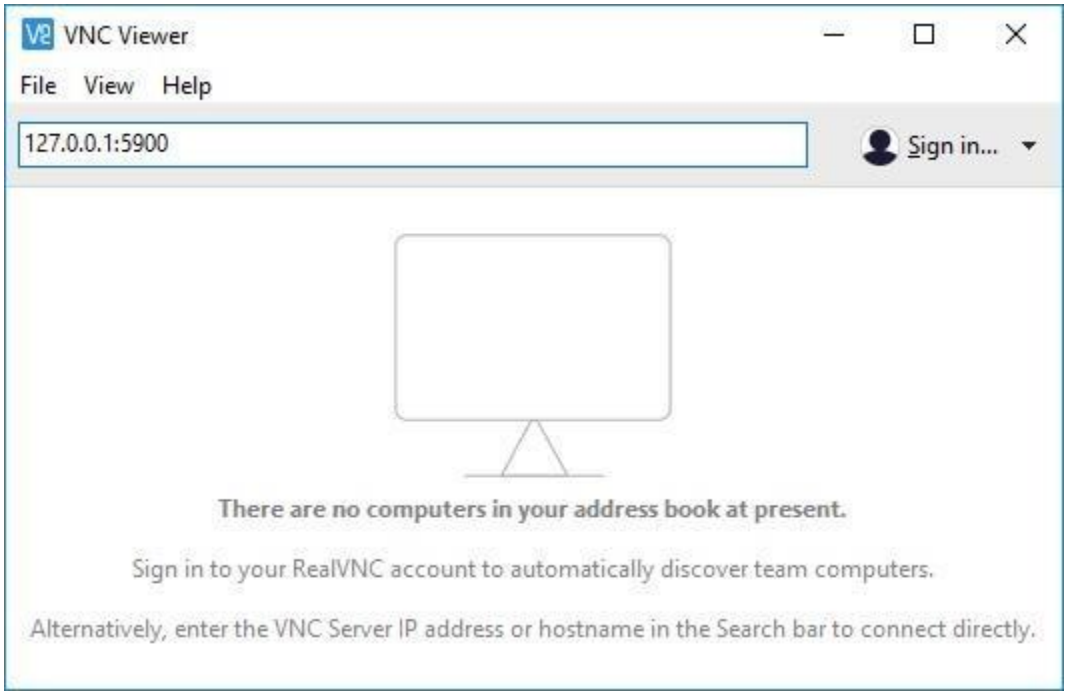


Figure 14 Using RealVNC Client with a local SSH tunnel

3. Press **Enter** or select the list item to connect.
4. Because the client is unaware of the encryption, it may show an inaccurate warning indicating that the connection is unencrypted. Click **Continue** to complete the connection.
   The VNC session to Server Host OS will be established over an encrypted channel.

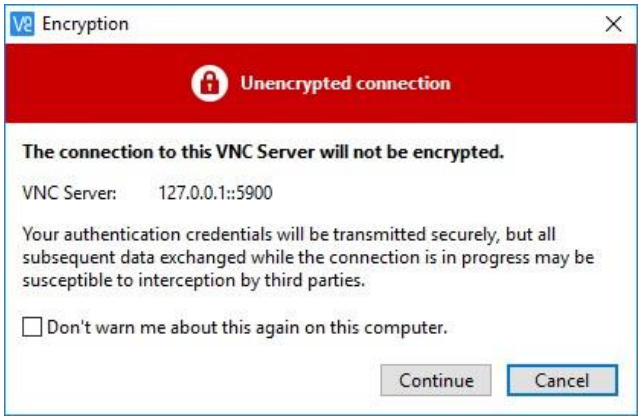


Figure 15 Unencrypted connection to the VNC server

5 Connecting Android with bVNC

The bVNC client supports secure VNC connectivity with iDRAC including VNC over SSH, and VNC over TLS. Both free- and donation-supported versions of the bVNC client are available from the Google PlayStore.

Dell OpenManage Mobile (OMM) is an application for provisioning, troubleshooting, and monitoring Dell servers. When bVNC is installed, OMM can read and configure iDRAC VNC settings, and launch bVNC with parameters to directly connect to the iDRAC VNC server. On the 14G servers equipped with the Quick Sync 2 module, OMM can activate Quick Sync Wi-Fi and start a wireless VNC session. It is recommended that you use OMM to launch bVNC when connecting to the PowerEdge servers. For resources with more information about OMM, see Technical support and resources.

5.1 Installing bVNC

To download and install bVNC from the play store:

1. Start the Google PlayStore 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. Click I**nstall**.

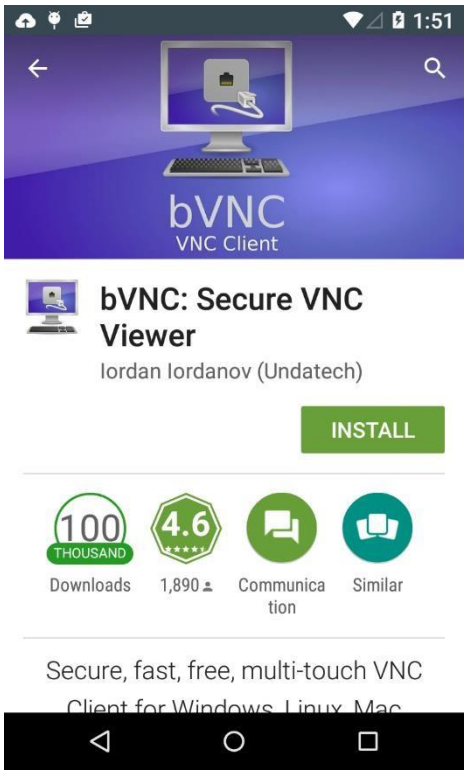


Figure 16 Installing bVNC

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

5.2 Connecting using bVNC

Prior to connection, the VNC server must be configured as specified in Configuring VNC by using the iDRAC GUI. To configure and establish a connection by using bVNC:

1. Start bVNC from the Android apps list or desktop.
2. In the **Connection Type** box:
   a. If using VNC over SSH to connect to a 14G server, select **Secure VNC over SSH**.
   b. If SSL Encryption is enabled in the iDRAC VNC Server settings, select **Secure VNC over SSL Tunnel**.
   c. Else, to connect without encryption, select **Basic VNC**.
3. If necessary, 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, type the iDRAC IP address or hostname. If using VNC over SSH, replace the default value of localhost, and also type the iDRAC IP address in the **SSH Server** box.
5. In the **Port** box, type the **VNC Port Number** from the iDRAC VNC Server settings.

Note—The default iDRAC VNC Port Number is 5901. Most VNC applications, including bVNC, display 5900 as the default port number, and it must be changed.

6. Configure your credentials:
   a. If using VNC over SSH, type an authorized iDRAC username and password in the respective **SSH Username** and **SSH Password** boxes.
   b. In the **VNC Password** box, type the same password as entered in the iDRAC VNC Server settings. If using VNC over SSH, this can be left blank.

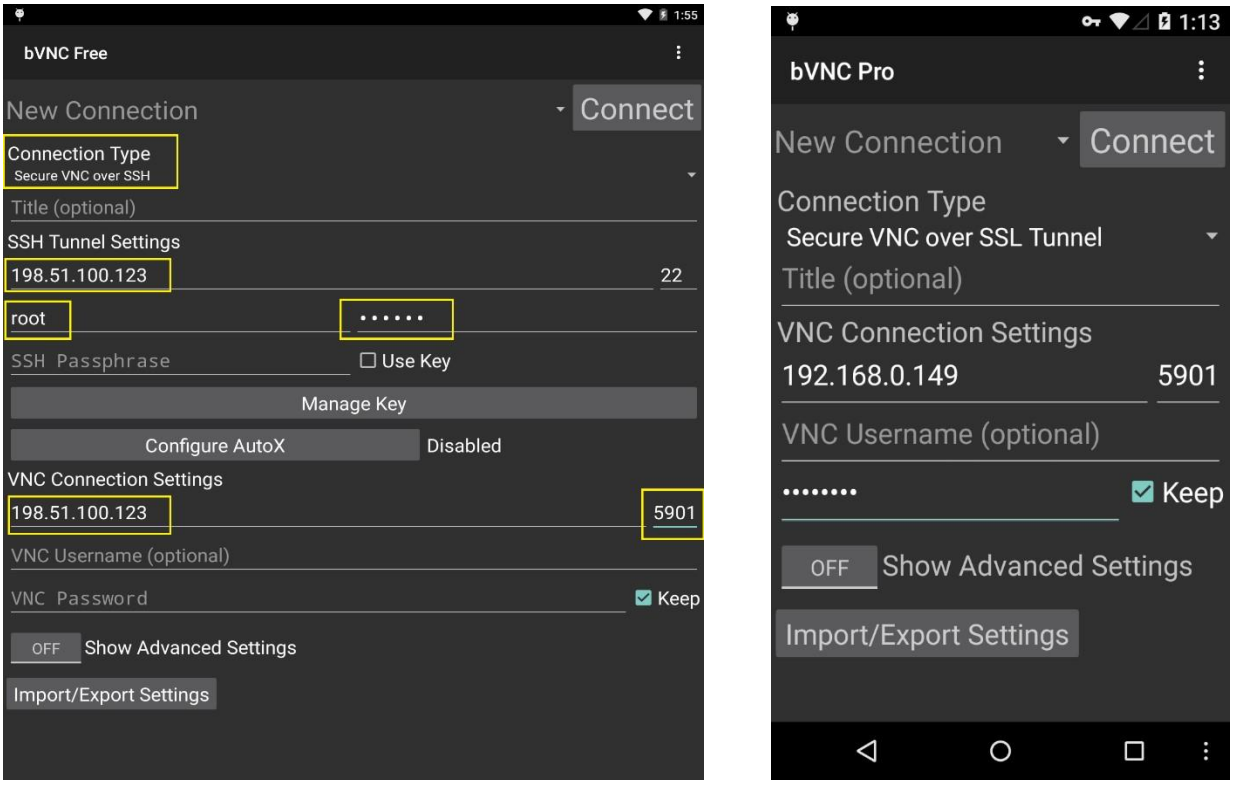


Figure 17 Connecting by using bVNC

7. Click **Connect** to start the VNC connection.
8. If using VNC over SSH, you will be prompted to accept the host public key. If TLS/SSL encryption is enabled, the certificate verification dialog box is displayed. Ensure that the certificate information corresponds to the expected iDRAC SSL certificate.
9. After verification, click **Yes**.
   The VNC session will be established.

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-controllerdrac-idrac

---

6 Connecting iOS with RealVNC Viewer, Remoter Pro, and Remotix

Remoter Pro and Remotix are remote desktop applications available for purchase in the Apple app store. They have support for VNC over SSH allowing secure connections to the 14G PowerEdge servers. RealVNC viewer is a free app available for download, but does not support encrypted connections the PowerEdge servers.

Dell OpenManage Mobile (OMM) is an app for provisioning, troubleshooting, and monitoring Dell servers. OMM can read and configure iDRAC VNC settings and, with a compatible VNC app installed, start a VNC connection to the iDRAC VNC server. On the 14G PowerEdge servers equipped with the Quick Sync 2 module, OMM can activate Quick Sync Wi-Fi and establish a wireless VNC session. It is recommended you use OMM to start VNC when connecting to the PowerEdge servers. For more information about OMM, see the Technical support and resources.

6.1 Installing RealVNC, Remoter Pro, or Remotix on iOS

To download and install a VNC app from the Apple app store:

1. Start the Apple *App Store* app from the home screen.
2. In the search box, type `RealVNC`, `Remoter Pro`, or `Remotix` to download the selected VNC client.
3. Click **Get** or ***Purchase***, and then click **Install**.

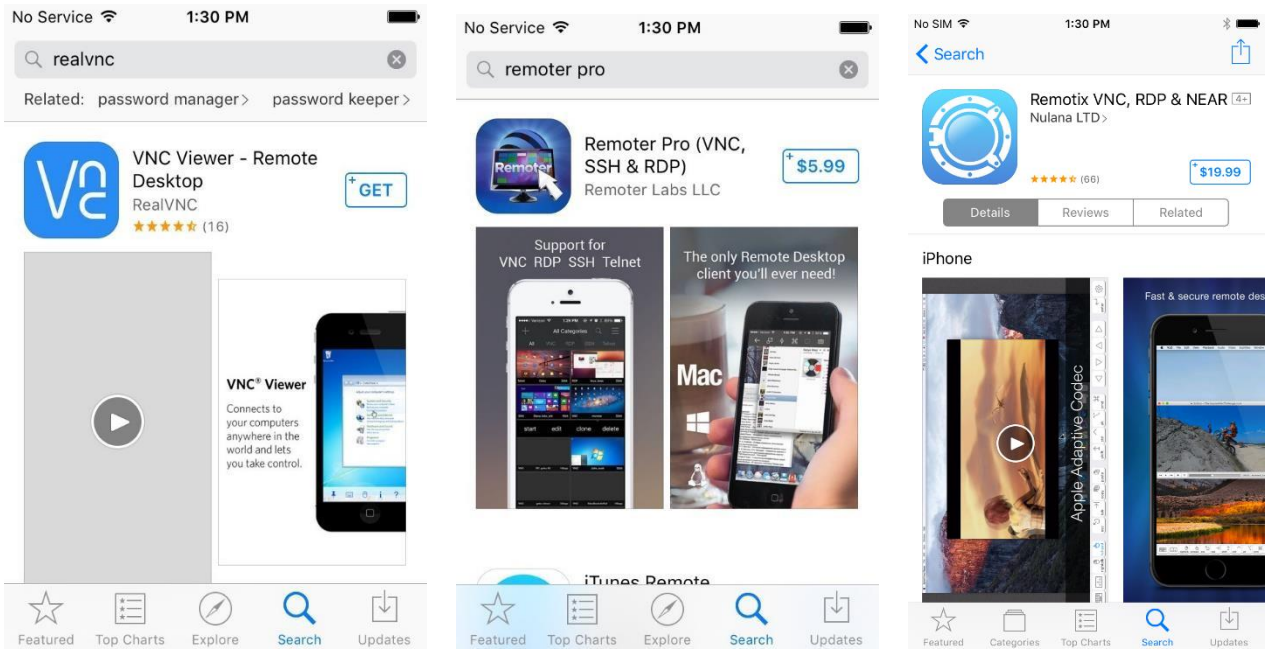


Figure 18 Installing RealVNC, Remoter Pro, or Remotix on iOS

6.2 Connecting using RealVNC Viewer for iOS

Prior to connection, the VNC server must be configured as specified in Configuring VNC by using the iDRAC GUI. To configure and establish a connection by using RealVNC Viewer for iOS:

1. Start RealVNC by double-clicking the desktop icon.
2. Click the **+** icon to add a connection to a known system.
3. Type the iDRAC IP and port number. For example, `198.51.100.123:5901`. Click **Next** and add an identifying name, if necessary.

Figure 19 Connecting using RealVNC Viewer for iOS

4. Click **Save** or **Done**.
5. Click **Connect**.
6. You will see a warning that the connection is unencrypted. Click **Connect** to proceed.
7. Enter the iDRAC VNC password when prompted.
8. The VNC session is established.

6.3 Connecting using Remoter Pro

Prior to connection, the VNC server must be configured as specified in Configuring VNC by using the iDRAC GUI. To configure and start a VNC over SSH connection by using Remoter Pro for iOS:

1. Start Remoter Pro from the desktop icon.
2. Press **+** to add a session.
3. Press **+** to manually add a session.
4. Under Server Type, select **VNC over SSH**.
5. Configure the session settings:
   a. Enter a session name
   b. Set the SSH Hostname to the iDRAC IP such as 198.51.100.123.
   c. Set the SSH Username and SSH Password to an authorized iDRAC username and password.
   d. Set the VNC Hostname to the iDRAC IP.

e. Change the VNC Port to the iDRAC VNC port (The iDRAC default is 5901).
f. Click **Save**.

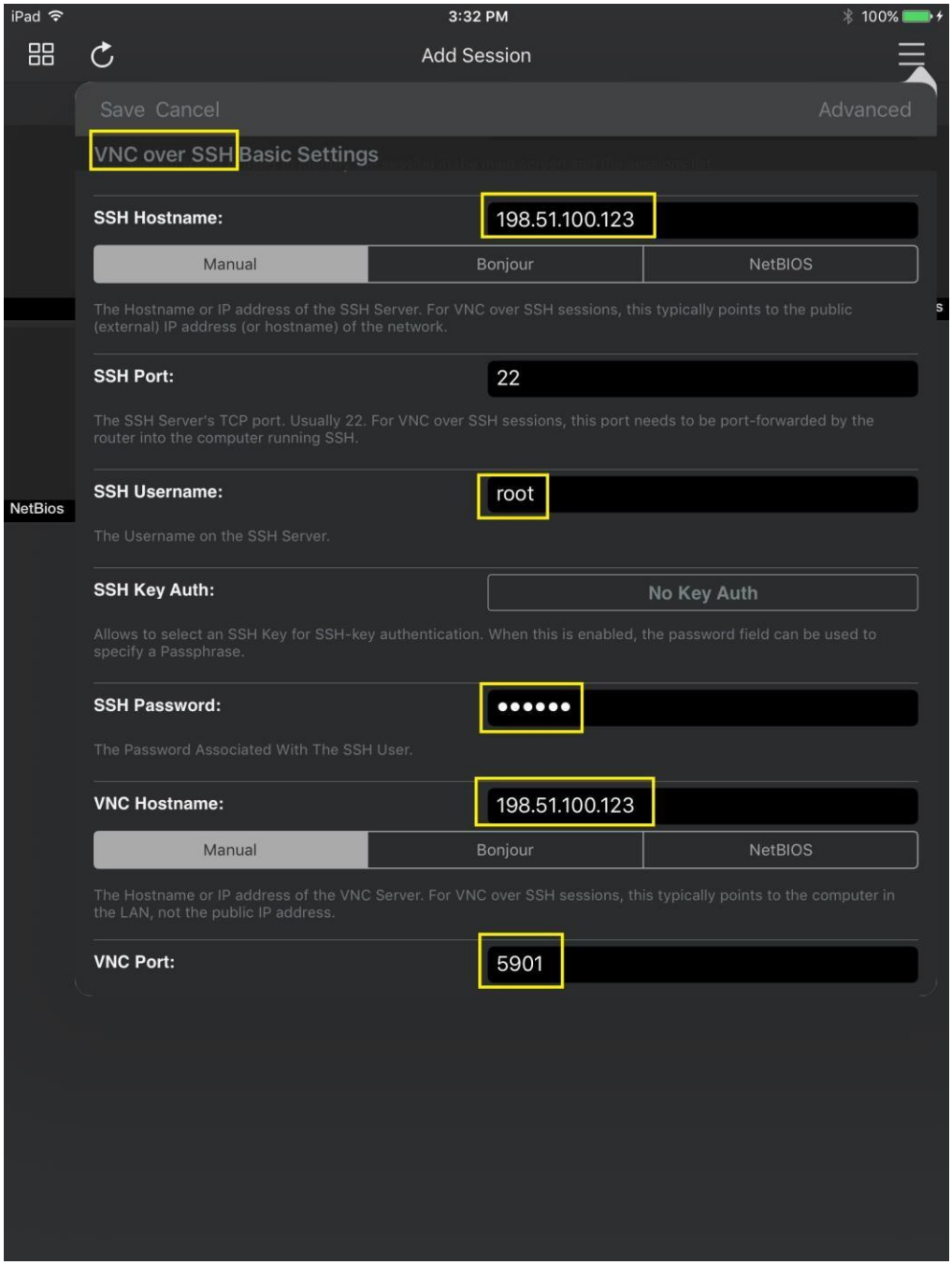


Figure 20 Connecting using Remoter Pro

6. Click the session entry, and click **Start**.
   The connection will be started.

6.4 Connecting using Remotix

Prior to connection, the VNC server must be configured as specified in Configuring VNC by using the iDRAC GUI. To configure and start a VNC over SSH connection by using Remotix:

1. Start Remotix from the desktop icon.
2. Tap the **+** icon to add a connection to a known system.
3. Select the Connection Type **VNC**.
4. Configure the connection settings:
    a. Enter a connection Name
    b. Set the connection Host to the iDRAC IP such as 198.51.100.123.
    c. Set the connection port to the iDRAC VNC port (The iDRAC default is 5901).

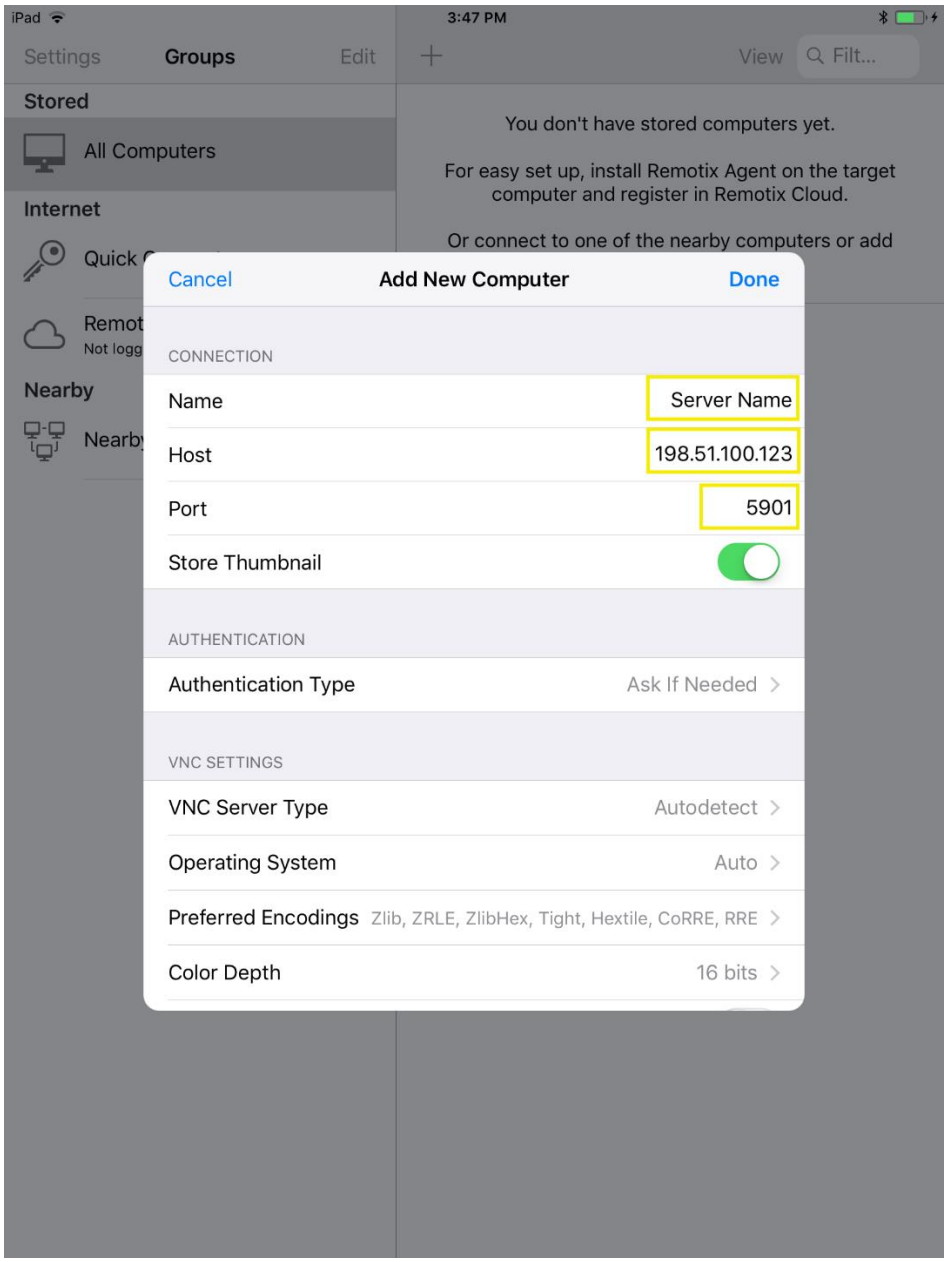


Figure 21 Connecting using Remotix

d. Configure the SSH tunnel
    i. Select the SSH Tunnel option and choose **Add new SSH Server**
    ii. Set the SSH Host to the iDRAC IP
    iii. Set the SSH username to an authorized iDRAC username
    iv. Make sure Authentication Type is set to **Password** and set the password to the iDRAC user's password

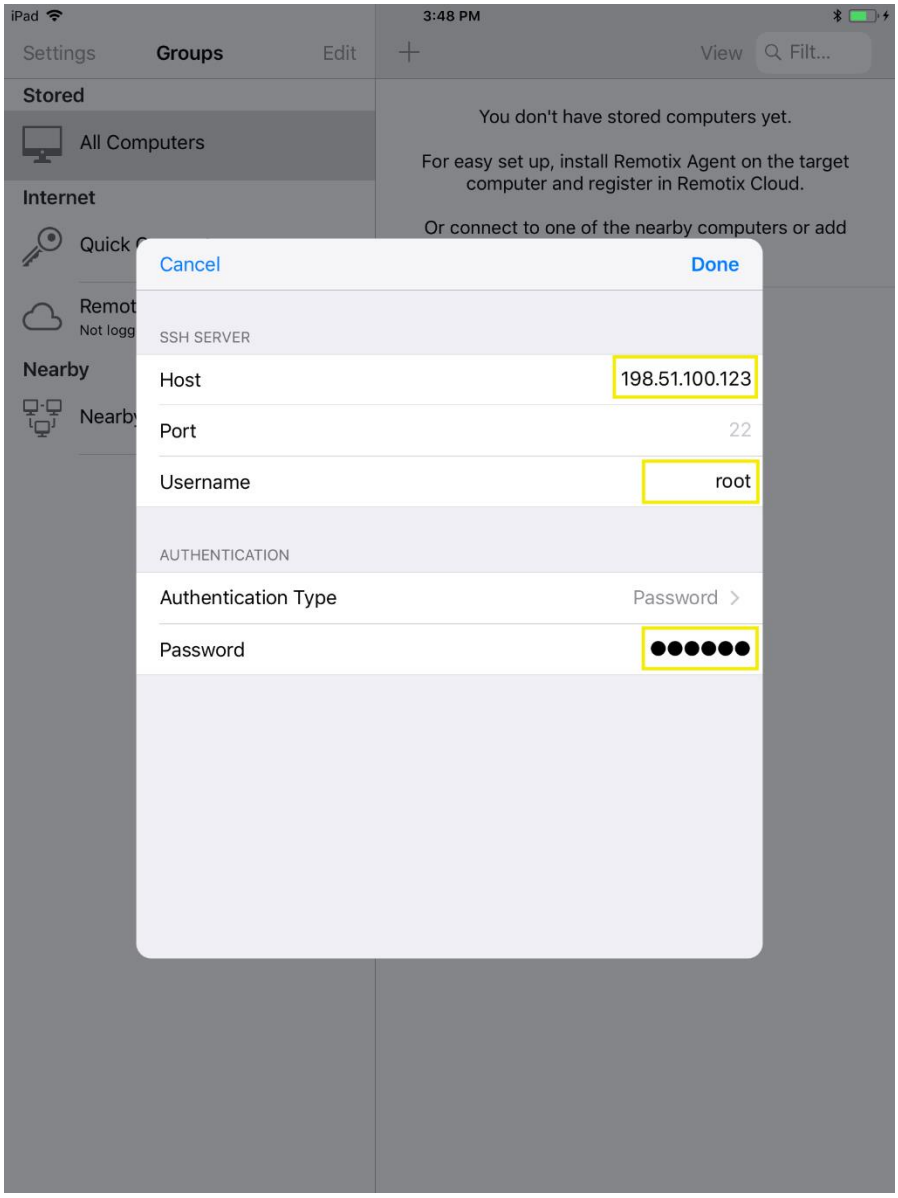


Figure 22 Connecting using Remotix—Add new SSH server

v. Tap **Done**
vi. Select the newly created SSH Server, and then tap the back button

e. Tap **Done**

5. Select the connection in the stored list.
   The connection will be started.

7 Accessing Virtual Media with VNC active

After the VNC session is started using any of the client, local media on a client such as a desktop or laptop can be mapped virtually to the server host OS by using the Virtual Media feature in iDRAC. This feature is useful where data must be made available remotely such as packages to update network drivers on the host OS.

7.1 Starting Virtual Media Redirection

1. Navigate to **Configuration → Virtual Console** on a 14G system, or **Overview → Server → Virtual Console** on a 13G and 12G system.
2. Click **Launch Virtual Console**.

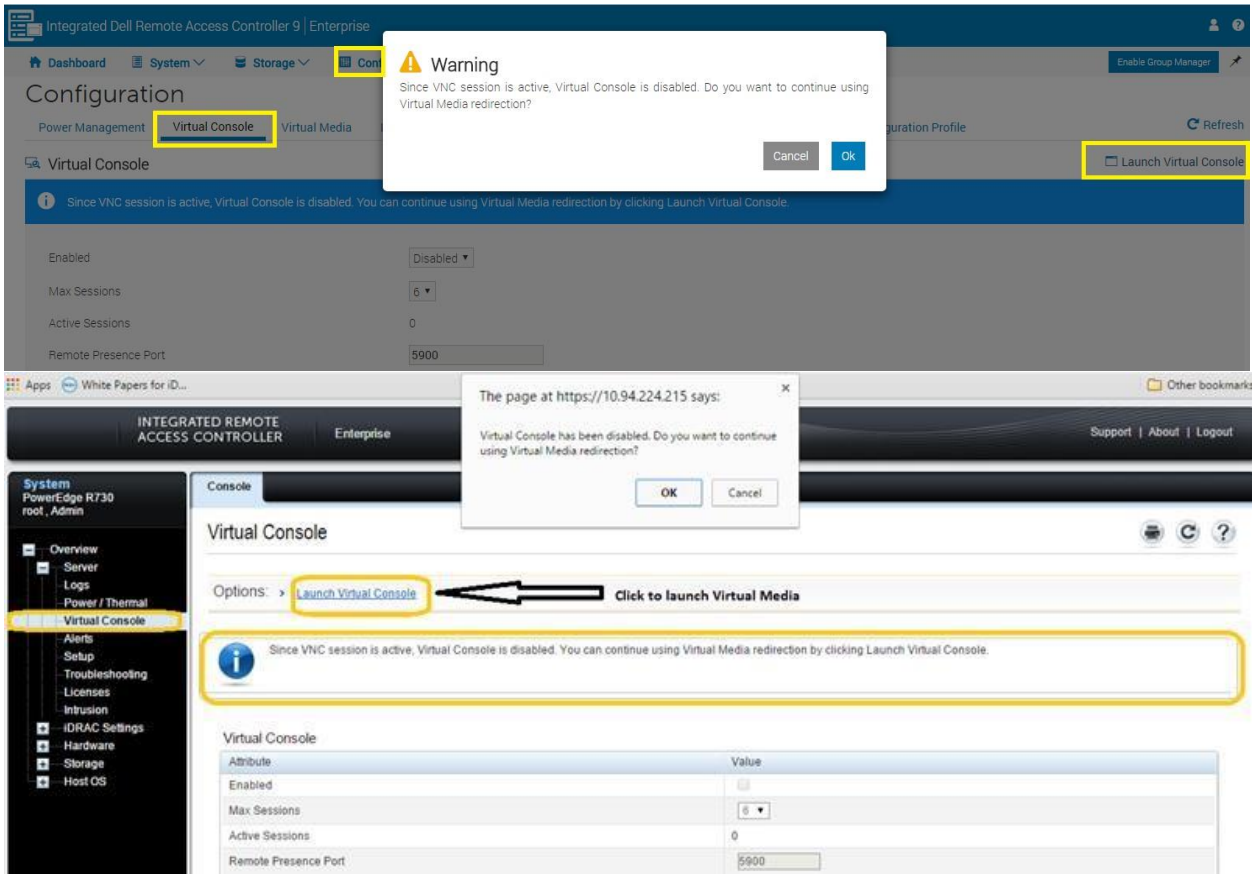


Figure 23 Starting Virtual Media Redirection

When prompted whether or not to continue using Virtual Media redirection,

3. Click **OK**.

When using Internet Explorer, an Activex plugin is start to launch the Virtual Media redirection utility.
Other browsers such as Chrome or Firefox, launch a Java applet.
You may be prompted to confirm the launch of Java, and then the launch of the applet.

4. Accept all prompts as required.

7.2 Mapping Virtual Media

To virtually map local media on to a server host OS:

1. On the **Virtual Media redirected** screen, click **Virtual Media**.
2. Select the required media mapping: either **Map CD/DVD** or **Map Removable Disk**.

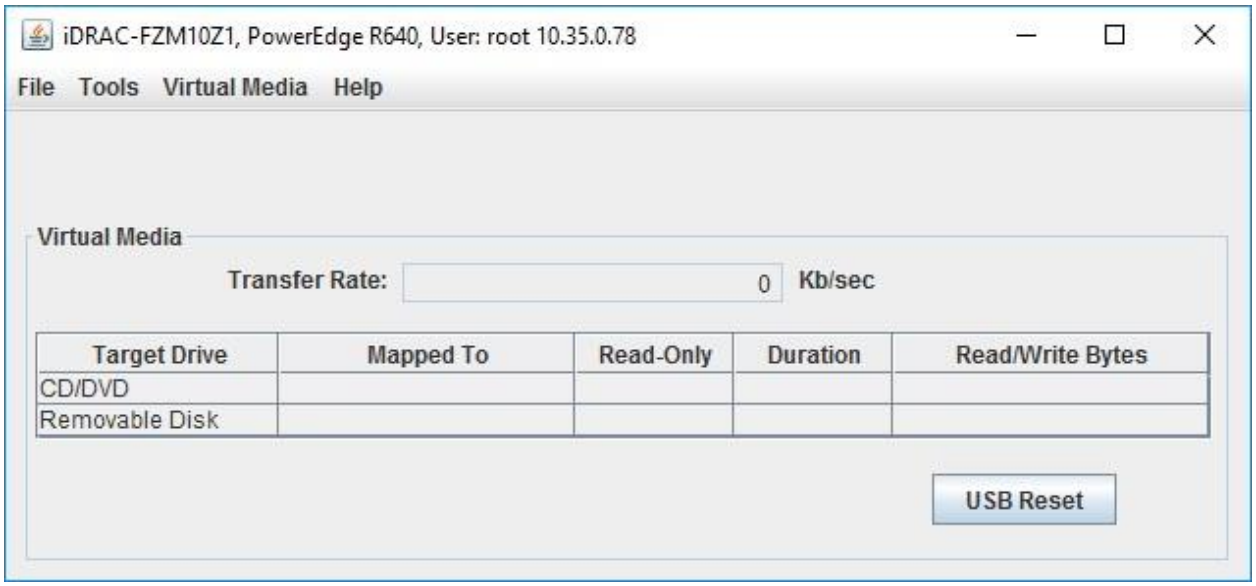


Figure 24 Starting Virtual Media Redirection—Mapping virtual media

The following example shows a mapped removable USB drive:

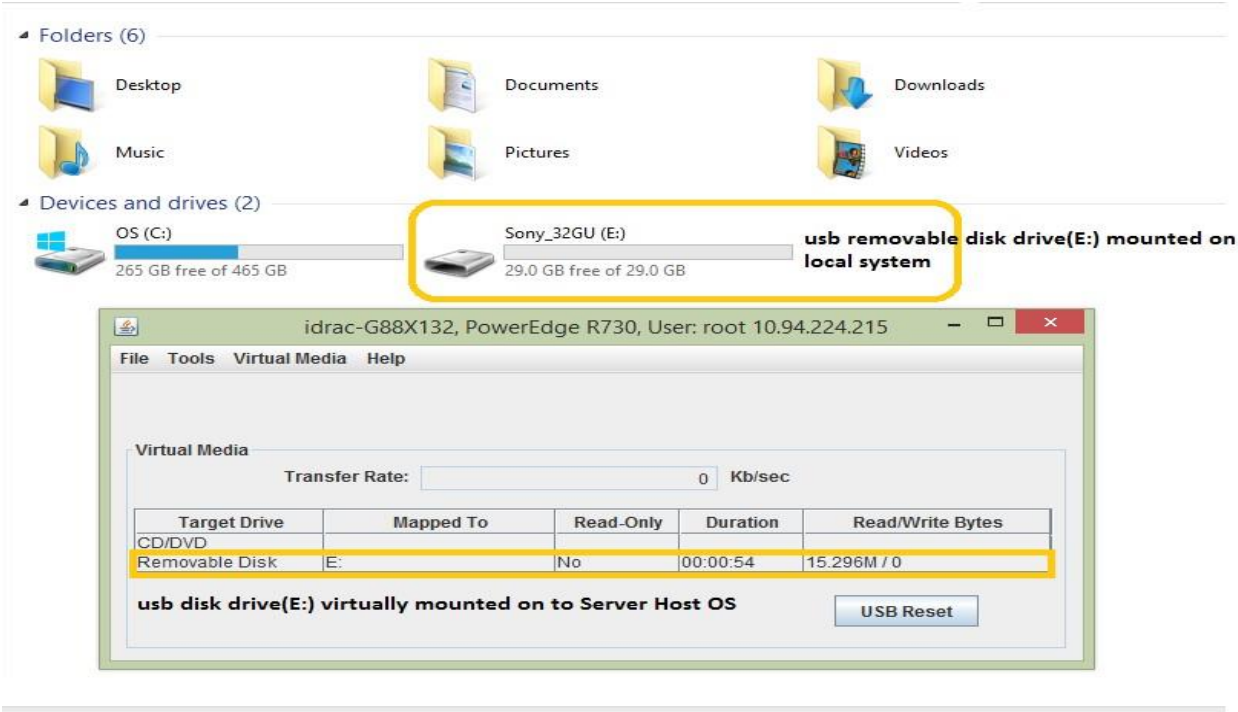


Figure 25

The mapped media can be seen in the Host OS:

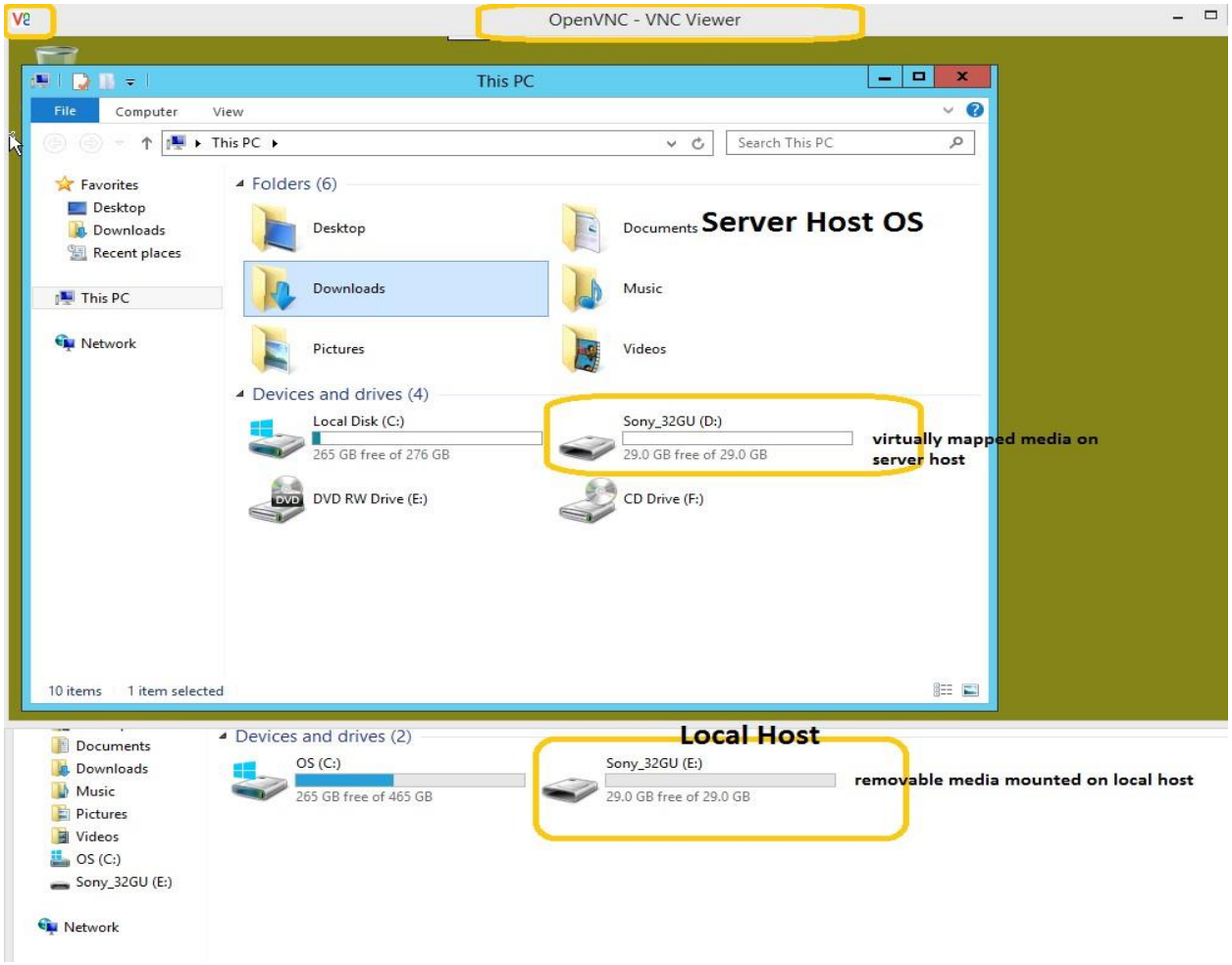


Figure 26

7.3 Unmapping Virtual Media

It is recommended that virtual media be ejected from the target host OS. Alternatively:

1. Click the mapped device in the **Virtual Media** list in the Virtual Media utility.
   The **Unmap Drive Requested** is displayed.
2. Click ***Yes*** to disconnect the virtual media.

8 Troubleshooting issues when accessing remote desktop using VNC

The following procedures assist in troubleshooting the VNC connectivity.

Symptom	Possible Causes	Resolution
Unable to connect to the iDRAC from VNC client	Settings are incorrect	Ensure that 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. If using VNC over SSH, do not enable TLS encryption. If tunneling, set the VNC client to use the ports required for tunneling.
	Network is unreachable	Ensure that: Network cables are attached Wi-Fi connection is available Required VPN connections are started 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.
	VNC client does not support iDRAC encryption	Switch to a VNC client that supports secure tunneling, or use an external secure tunneling program such as 'ssltunnel'. It may be useful to attempt to connect to the iDRAC with 'encryption' disabled.
Lost VNC connection to VNC server	VNC session timeout	VNC session remains active until session timeout period is configured in the iDRAC VNC server settings. Allowed session timeout period range is 60–10800 seconds.
	Host system power cycled and with iDRAC NIC in shared mode.	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 restart the VNC connection.
	VNC Client window minimized for more than 60 seconds	If the VNC client window is minimized for more than 60 seconds, the client window closes. You must start a new VNC session. If you maximize the VNC client window within 60 seconds, you can continue using it.
VNC server displays active sessions, when no clients are actually connected. Unable to connect to iDRAC from VNC client.	VNC server state is invalid	Reset the iDRAC. Alternatively, disable and reenable the VNC server by using the iDRAC GUI. Consider reducing the VNC Server timeout value. Ensure the latest firmware is installed.
VNC client indicates that the video is corrupted	VNC client is not compatible	Use a known compatible client such as those listed in this technical white paper.

Technical support and resources

- Dell.com/support is focused on meeting customer needs with proven services and support.

A.1 Related resources

- Information on the SSVNC client is available at:
- http://www.karlrunge.com/x11vnc/ssvnc.html
- Information on Dell OpenManage Mobile is available from: http://en.community.dell.com/techcenter/systems-management/w/wiki/4965.openmanage-mobile
- bVNC can be downloaded from the Google Play store at: https://play.google.com/store/apps/details?id=com.iiordanov.freebVNC&hl=en
- RealVNC Viewer for iOS is available from the Apple App Store https://itunes.apple.com/us/app/vnc-viewer-remote-desktop/id352019548?mt=8
- Remoter Pro for iOS is available from the Apple App Store https://itunes.apple.com/us/app/remoter-pro-vnc-ssh-rdp/id519768191?mt=8