

Honeywell

Experion PKS Technical Note # 395

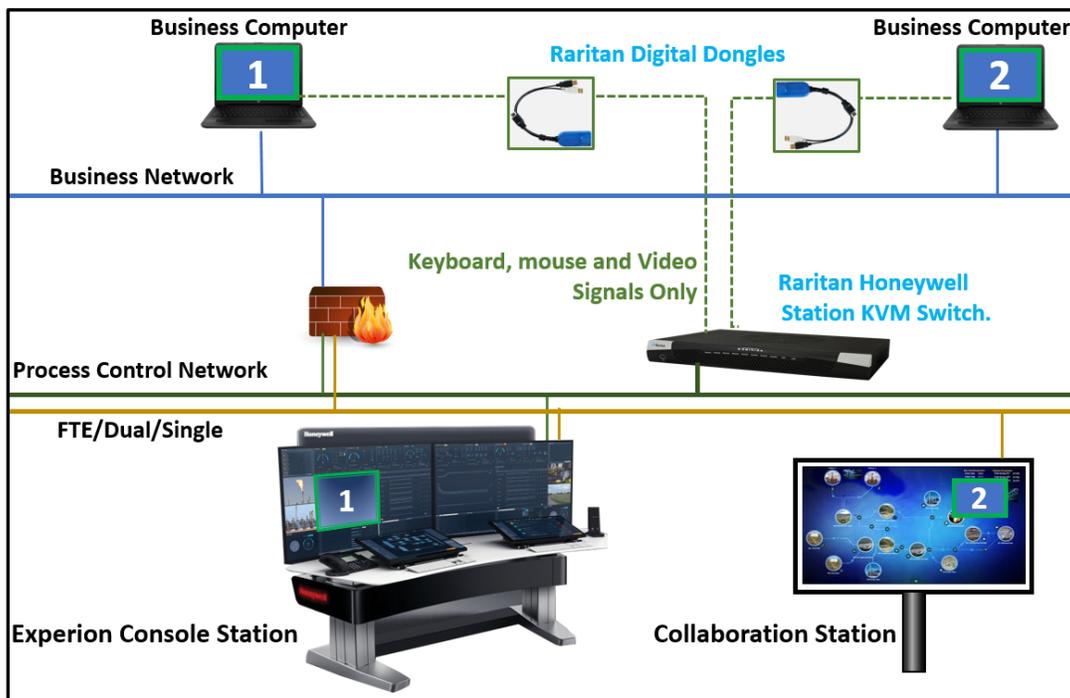
Date: August 27, 2019
Issued By: Technology
Subject: Experion Raritan KVM Client Configuration and Operation
Release: Experion R500, R510, R511
Applicable to: Experion
Keywords: Business, Station, Collaboration, Orion, Raritan KVM
Distribution: For Projects, TAC, and Customers

1 Purpose

This technote describes how to use the Experion Raritan KVM Client to securely connect to Windows OS business computers from Experion Stations, such as Orion Console Stations and Collaboration Station, on the Process Control Network.

1.1 About the Experion Raritan KVM client

The Experion Raritan KVM client provides secure, high definition access from Experion Stations on a Process Control Network to computers on the business network.



No network access is required, and no firewall ports need to be opened between the business network and the Process Control Network. Keyboard, video and mouse signals are transmitted between the business computer and Experion Stations via the Raritan KVM hardware and the Experion Raritan KVM client. The Experion Raritan KVM Client provides a Microsoft Remote Desktop-like user experience supporting full High Definition resolution at up to 30fps.

NOTE: Only one network port on the Raritan Switch needs to be connected to the Process control network, as illustrated in the topology diagram above.

One license is required for each Experion Raritan KVM client, as shown here:

Model Number	Description
EP-EKVMC1	Experion Raritan KVM Client (1 client license)

2 Connect and configure the Raritan KVM hardware

This section outlines how to set up and configure the Raritan hardware with Experion Stations. For more detailed information, see the [Raritan KVM online documentation](#).

The steps involved with connecting and configuring the Raritan KVM hardware are:

1. [Connecting the Raritan KVM switch](#)
2. [Configuring the KVM switch](#)
3. [Configuring authentication settings](#)
4. [Configuring user profiles](#)
5. [Configuring security settings](#)
6. [Setting viewing resolution](#)
7. [Configuring the business PC to lock when disconnected](#)
8. [Configuring the business PC to enable concurrent access by multiple users](#)

2.1 Connecting the Raritan KVM switch

The following Raritan KVM hardware can be purchased from your regional Raritan reseller.

KVM Switch	A Raritan Honeywell Experion Station KVM switch is required to connect business computers to Experion Stations on the Process Control Network.	
	Model Number	Description
	DKX3-808-HWES	<ul style="list-style-type: none">• Honeywell Experion Station Supported KVM-over-IP switch, for 8 x Single Display Business PC, Local Admin Port and Audio support for Business PC Network. Dual Power Supply and Dual Gigabit LAN, includes 2 Years Hardware Warranty.• Number of business network computers accessible: 8• Number of concurrent Raritan KVM clients supported: 8
Digital Dongle	A Raritan digital dongle is required to connect business computers to the Raritan Honeywell Experion Station KVM switch. One dongle is required for each business computer. Select the dongle below based on the video output available on the business computer.	
	Model Number	Description
	D2CIM-DVUSB-DP-HWES	Business PC Computer Interface Modules with USB & Display Port Video for use with DKX3-808-HWES. (Supports Audio)
	D2CIM-DVUSB-DVI-HWES	Business PC Computer Interface Modules with USB & DVI Video for use with DKX3-808-HWES. (Supports Audio)
	D2CIM-DVUSB-HDMI-HWES	Business PC Computer Interface Modules with USB & HDMI Video for use with DKX3-808-HWES. (Supports Audio)

To connect the Raritan KVM switch:

1. Connect the switch to the Process Control Network.
2. Attach an appropriate Raritan Digital Dongle to each business PC that you want to access from your Experion Stations.
3. Connect each Raritan Digital Dongle to the Raritan KVM Switch with an ethernet cable.

2.2 Configuring the Raritan KVM switch

1. Connect a keyboard, a mouse, a monitor, and a power cord to the Raritan KVM switch and power up the switch.
2. Log into the switch using the following default credentials:

Option	Value
Username	admin
Password	Raritan
IP address	192.168.0.192

Note: You will be prompted to change the default password after your initial Signon, however, Honeywell recommends that KVM switch credentials not be stored so as to ensure each KVM client connection is individually authenticated by the user.

3. From the Home page, choose **Device Settings > Network** to display the **Basic Network Settings** page.
4. Enter the **IP address** and **DNS** settings relevant for your network, then click **OK**. For more information, see <https://help.raritan.com/kx-iii/v3.5.0/en/#2658.htm>.
5. Under the LAN Interface section, ensure that the Speed and Duplex settings match those for the FTE Switch. Default is 'Automatic'.
6. Choose **Device Settings > Port Configuration** to display the **Port Configuration** page.

Port Access	Power	Virtual Media	User Management	Device Settings	Security	Maintenance	Diagnostics	Help
Home > Device Settings > Port Configuration								
Port Configuration								
▲ No.	Name	Type						
1	PC1	DVM-HDMI						
2	PC2	DVM-HDMI						
3	Dominion_KX3_Port3	Not Available						
4	Dominion_KX3_Port4	Not Available						
5	Dominion_KX3_Port5	Not Available						
6	Dominion_KX3_Port6	Not Available						
7	Dominion_KX3_Port7	Not Available						
8	Dominion_KX3_Port8	Not Available						

- Click on each port to which you have connected a business PC, and rename it to a more meaningful name. (It does not necessarily have to be the same name as the business PC). You will use this name to connect to the business PC from an Experion Station. Names must be unique, and be less than 32 characters long.

Note: By default, the KVM Client sets the port name as the window title. Port names must be unique so that SafeView placeholders can be configured using port names as category match criteria. When used with SafeView, the KVM Client window displays a maximum of 15 characters of the business PC name, and provides a tooltip containing the full name.

- From the KVM Client home page, choose **Device Settings > Device Services**.
- Set the HTTPS port number to **443**, then click **OK**.

This is the port number by which Experion Stations will communicate with the KVM Switch.

2.3 Ensuring the Raritan KVM switch security

2.3.1 Configuring SSL certificates

The Raritan KVM switch uses SSL certificates to ensure connection security. The certificates can be either Certificate Authority-Signed or Self-signed. A Certificate Authority-Signed certificate is the preferred option, and can be obtained from a third party or an internal Certificate Authority. If this is not feasible, a Self-Signed certificate must be installed on the KVM hardware.

This section provides instructions for both options.

To configure a Certificate Authority-Signed certificate:

- From the KVM Client home page, choose **Security > Certificate**.
- Complete the following fields:

Field	Value
Common Name	The network name of the KVM switch on your network (fully qualified domain name).
Organization Unit	The department that owns the KVM switch within the organization.
Organization	The name of the organization.
Locality/City	The city in which the organization is located.
State/Province	The state in which the organization is located.
Country (ISO code)	The two-letter code for the country in which the organization is located.
Challenge Password	If required by your certification authority, the password required to change the certificate.

Confirm Challenge Password	Confirmation of the challenge password.
Email	The email address of the person responsible for the KVM switch in your organization.
Subject Alternative Name	Same as common name.
Key Length	The length of the generated key, in bits. 1024 if the default length, and a maximum of 4096 bits is supported.

3. Click **Create** to generate a Certificate Signing Request (CSR).

A message summarizing the details you have provided appears. Review this, and click **Download**.

4. Email the CSR to the certifying authority for certification as per your standard IT certification policies.
5. When you receive the certificate, click **Upload** to upload the certificate to the KVM switch.
6. Reboot the KVM switch to activate the certificate.

To configure a self-signed certificate:

1. From the KVM Client home page, choose **Security > Certificate**.
2. Complete the following fields:

Field	Value
Common Name	The network name of the KVM switch on your network (fully qualified domain name).
Organization Unit	The department that owns the KVM switch within the organization.
Organization	The name of the organization.
Locality/City	The city in which the organization is located.
State/Province	The state in which the organization is located.
Country (ISO code)	The two-letter code for the country in which the organization is located.
Challenge Password	If required by your certification authority, the password required to change the certificate.
Confirm Challenge Password	Confirmation of the challenge password.
Email	The email address of the person responsible for the KVM switch in your organization.
Subject Alternative Name	Same as common name.

Key Length	The length of the generated key, in bits. 1024 if the default length, and a maximum of 4096 bits is supported.
-------------------	--

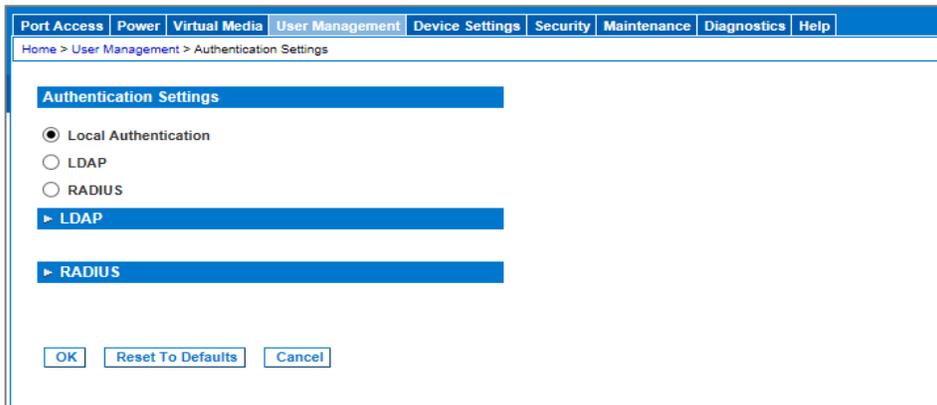
3. Select the Create a Self-Signed Certificate check box, then click **Create**, which means that the KVM switch will create the certificate and act as the certifying authority.
4. Specify a number of days for which the certificate will be valid, then click **Create**.
5. Click **OK** to dismiss the confirmation message when it appears.
6. Reboot the KVM switch to activate the certificate.

Next steps: [Install the SSL certificate on every Experion Station](#) that will communicate with the KVM hardware.

2.4 Configuring authentication settings

To set the KVM Client authentication:

1. From the KVM Client home page, choose **User Management > Authentication Settings**.
2. From the Authentication Settings page, select Local authentication, then click OK.



2.5 Configuring user profiles

The Raritan KVM switch stores an internal list of all user profiles and user groups to control access authorization and permissions. All users must therefore be authenticated to be able to access the Raritan KVM switch.

2.5.1 Creating a new user group

User groups control access permissions. Honeywell recommends creating a group for each type of user access required.

1. From the KVM Client home page, choose **User Management > Add New User Group**.
2. From the **Group** page, add a **Group Name**, then apply the following options:
 - **Permissions:** leave all options unselected

- **Port Permissions:** for each connected business PC, set the **Access to Control**, **VM Access** to **Deny**, and **Power Control** to **Deny**.

3. Click **OK**.
4. Repeat these steps for any other groups you need to create.

For more information about the Raritan KVM Client permission settings, see the [Raritan online help](#).

2.5.2 Adding new users

1. From the KVM Client home page, choose **User Management > Add New User**.
 2. From the **User** page, add a **Username** and **Password** for the new user.
 3. From the **User Group** list, select the group to which you want to add this user, then click **OK**.
- Note:** To activate users, the **Active** check box must be selected.

2.6 Configuring security settings

1. From the KVM Client home page, choose **Security > Security Settings**.
2. From the **Security Settings** page, apply the following settings:

Option	Recommended setting
Login Limitations > Enable Password Aging	Selected. This prompts users to change their passwords periodically, according to the value entered into the Password Aging Interval (Days) field.
Encryption & Share > Encryption Mode > Enable FIPS 140-2 Mode	Selected. After FIPS mode is activated, a new SSL certificate must be created to complete the FIPS Mode-compliant requirements. See Security Considerations for more information.

2.7 Setting the business PC viewing resolution

1. From the KVM Client home page, choose **Device Settings > Port Configuration > Port**.
2. For each connected business PC, under **Target Settings**, select the appropriate resolution from the **Display Native Resolution** list.

For example, if the business PC video driver supports a maximum resolution of 1920 * 1200 at 60hz, set the **Display Native Resolution** to 1920 * 1080@60hz.

2.8 Configuring the business PC to lock when disconnected

The `WinLock_OnDisconnect` connection script can be used to automatically lock the business PC when it has no active connections.

To configure the business PC to lock when disconnected:

1. From the KVM Client home page, choose **Device Settings > Connection Scripts**.
2. Click **Import**.
3. Locate and select `WinLock_OnDisconnect.xml`, then click **Import**.
4. From the Available Connection Scripts, select `WinLock_OnDisconnect.xml`.
5. From the Apply Selected Scripts to Ports section, select the target(s) to which to apply the disconnect script.
6. Click **Apply Scripts**.

Note: If the business PC share is in *shared mode*, the disconnect script will only be executed when all connections are terminated.

2.9 Configuring the business PC to enable concurrent access by multiple users

PC sharing enables multiple users to access and view the content of a business PC at the same time.

To enable sharing of the business PC:

1. From the KVM Client home page, choose **Security > Security Settings**.
2. From the **Encryption & Share** section, set **PC Share Mode** to **PC-Share** and select **VM share Mode**.
3. From the KVM Client home page, choose **User Management > User Group List**.
4. Choose the user group requiring share access to the business PC, then set the **Permission** for that group to **PC-share**.

3 Setting up Experion Stations

This section outlines how to set up and configure the Experion Stations that will be used to access the business PCs through the Raritan hardware.

The steps involved with setting up the Experion Stations are:

1. [Installing the SSL certificate](#)
2. [Installing and configuring the Experion Raritan KVM Client software](#)
3. [Configuring the Experion Station](#)

3.1 Installing the SSL certificate

1. From a browser window on the Experion Station, navigate to **https://<KX III IP address>/**, where *<KX III IP address>* is the IP address of the Raritan KVM switch.
2. Click to **Continue to this website**, and click **Yes** at any security alert windows that appear.
3. At the KVM login page. Enter the user credentials created during the KVM Hardware configuration, then click **Login**.
4. From the KVM Client home page, choose **Security > Certificate** to display the **SSL Server Certificate Management** page.
5. From the Certificate Upload section, click Download Current Certificate.
6. Save the certificate as **RaritanKVM.cer**, then right-click on the certificate and click **Install Certificate** to launch the **Certificate Import Wizard**.
7. Select **Local Machine**, then click **Next**.
8. Select Place all certificates in the following store, then click Browse.
9. Select Trusted Root Certification Authorities, then click OK.
10. Click **Finish** to complete the certificate installation.

3.2 Installing and configuring the Experion Raritan KVM Client software

Pre-requisites:

- Administrative privileges on the Experion node
- Station has been installed
- ExperionRaritanKVMClient.zip has been downloaded from honeywellprocess.com/library/support/software-downloads/Experion/ExperionRaritanKVMClient.zip, and the following files have been extracted to a folder on the Experion node
 - ExperionRaritanKVMClientInstaller.exe (the installation file)
 - WinLock_OnDisconnect.xml (a script enabling automatic locking of the business PC on disconnect)
 - SVRTN395.PDF (this document)
 - Sample_KVM4K_4x1600x900R_FP.wdl (a sample SafeView workspace configuration file)

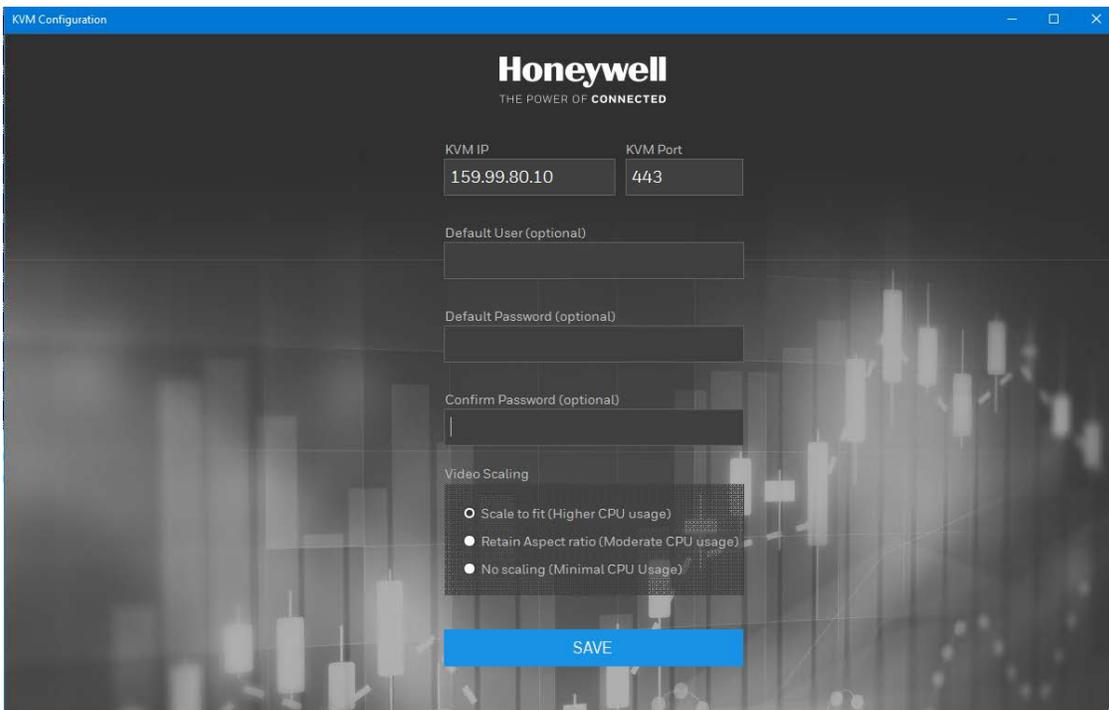
To install the Raritan KVM Client software:

1. From the folder containing the extracted software zip file, right-click on the installer file and select **Run as Administrator**.
2. Provide credentials if prompted, and follow the wizard instructions to complete the installation.

The Experion Raritan KVM Client software is installed in the default Station installation path.

To configure the Experion Raritan KVM Client settings:

1. From a command prompt with Administrator privileges, navigate to the following directory:
<Experion installation path>\Honeywell\Experion PKS\Client\Raritan
2. Type `ExperionRaritanKVMClient.exe -conf`, then press **Enter** to display the KVM Configuration window.



3. Enter the **KVM IP**, **KVM Port**, **User** and **Password** details as configured earlier in [Connect and configure the Raritan KVM hardware](#).

Note: The **User** and **Password** fields are optional. For enhanced security it is recommended that these be left blank so that users are prompted to enter their own credentials when connecting to the business PC.

4. Select an appropriate scaling option from one of the following:

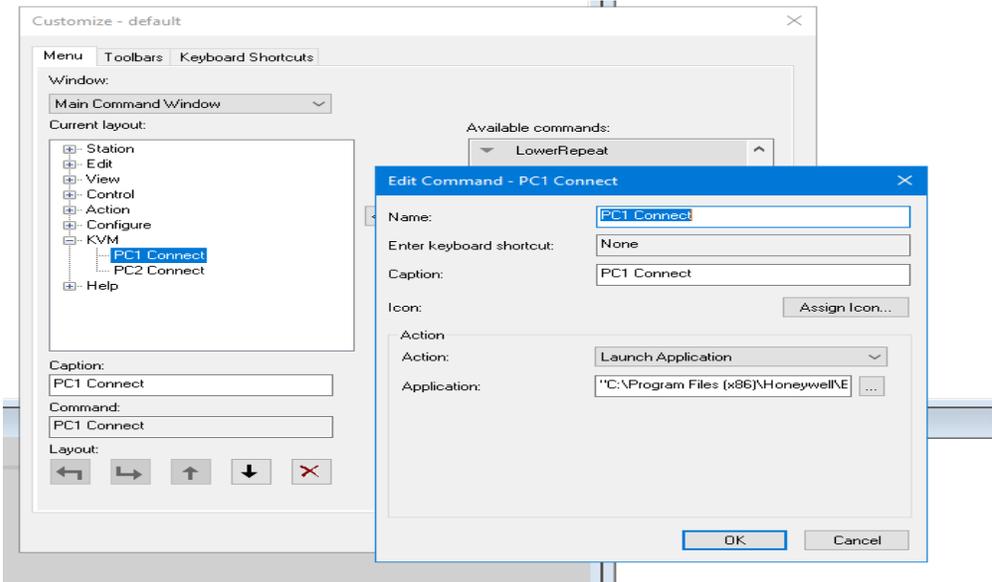
Option	Description
Scale to fit (Higher CPU usage)	The business PC content is scaled to fit the viewing window. CPU usage is higher with this option.
Retain Aspect ratio (Moderate CPU usage)	The business PC content is scaled to fit the viewing window while also retaining the same aspect ratio. CPU usage is moderate with this option.
No scaling (Minimal CPU usage)	The business PC content is displayed at the same resolution as is set on the business PC. If the business PC resolution is higher than what can be displayed on in the viewing window, scroll bars will be introduced. CPU usage is minimal with this option.

3.3 Configuring the Experion Station

This section lists the additional tasks required to securely integrate content from the business PC to Experion Stations.

3.3.1 Configuring Station to launch the Experion Raritan KVM Client

1. From Station, choose **Station > Connection** properties.
2. From the **Toolbar** tab, choose **Menu > Toolbar and Keyboard Shortcuts**.
3. Select the **.stb** file you want to customize, then click **Customize**.
4. From the **Menu** tab, select **Heading** and click **Insert**.
5. Change the heading to **KVM**.
6. Click **New command** to display the **Edit Command** dialog.
7. Enter a **Name** for the command, for example **PC1 Connect** (as shown here).



8. From the **Action** list, choose **Launch Application**, then add the *Application* path details. For example: "<Experion install path>\Honeywell\Experion PKS\Client\Raritan\ExperionRaritanKVMClient.exe" "<Port_Name>"

Where <Port_Name> is the name of the port you configured earlier in [Connect and configure the Raritan KVM hardware](#).

9. Repeat these steps for every business PC you will be accessing from this Station.
10. Use the arrow keys to move the new Station menu items to the desired position in the menu.
11. Save the file as a new *.STB* file.

3.3.2 Configuring SafeView for Orion Console and Multi-Window Stations

The Experion Raritan KVM Client uses the port name as the window title, and can be used as a SafeView placeholder.

To manage multiple KVM Clients in a SafeView placeholder, you need to add a match expression to the WDL file.

Example 1: This example is using "?*PC?*" as the window title:

```
window UpperRightWindow
  match = |title("?*PC?*");
  position = TG_xposition, TG_yposition;
  size = TG_xsize, TG_ysize;
  closable = yes;
  sizeable = yes;
  placeholder = yes;
  always on top = no;
  minimizable = no;
  maximizable = no;
  titlebar = no;
end window
```

Example 2: This example is using the same window title as example 1, but the placeholder is also shared with System Group and System Trend windows:

```
window UpperRightWindow
  match = category ("HW_System_Trend") or category ("HW_System_Group") or title("?*PC1?*");
  position = TG_xposition, TG_yposition;
  size = TG_xsize, TG_ysize;
  closable = yes;
  sizeable = yes;
  placeholder = yes;
  always on top = no;
  minimizable = no;
  maximizable = no;
  titlebar = no;
end window
```

You can modify the SafeView workspace according to operator preference and in line with other console configuration requirements. As the KVM Client uses the port name as the window title by default, Honeywell recommends that you configure a generic placeholder as shown here to catch any unexpected error dialogs that may be generated by the KVM switch.

```

window UpperLeftWindow
  match = category ("?*");
  position = AS_xposition, AS_yposition;
  size = AS_xsize, AS_ysize;
  draggable = AS_draggable;
  closable = yes;
  sizeable = yes;
  placeholder = yes;
  always on top = no;
  minimizable = no;
  maximizable = no;
  tabwindow = no;
  titlebar = no;
end window

```

3.3.3 Configuring Collaboration Station to connect to the business PC

To connect to a business PC from a Collaboration Station, you need to perform some additional steps.

1. Using a text editor, modify the radial menu JSON file as shown here:

```

{
  "displays": [],
  "documents": [
    {
      "name": "Port_name",
      "path": "C:\\Program Files (x86)\\Honeywell\\Experion
        PKS\\Client\\Raritan\\ExperionRaritanKVMClient.exe <Port_name>",
      "id": 0
    },
    {
      "name": "PC1",
      "path": "C:\\Program Files (x86)\\Honeywell\\Experion
        PKS\\Client\\Raritan\\ExperionRaritanKVMClient.exe PC1",
      "id": 1
    }
  ],
  "people": [],
  "workspace": []
}

```

Where <Port_name> is the name of the port configured earlier in [Configuring te Raritan KVM switch](#).

2. From the **Radial** menu, click on the Business PC option and provide credentials if prompted.
The business PC content appears as a content window in Collaboration Station and can be resized and repositioned as required.
3. Click **Ctrl + Alt + Del** in the content window Control Panel to log into the business PC.

4 Accessing the business PC from an Experion Station

The Experion Raritan KVM client provides secure access to business network applications, such as email, operations document systems, and intranet and internet applications, from Experion Stations on the process control network. Business applications remain securely hosted on the business network while secure interaction occurs through the transmission of keyboard, video and mouse signals only. The Experion Raritan KVM Client is certified for use with SafeView in Orion Consoles and Multi-Window Stations.

Prerequisites:

- [Configured SafeView workspace](#)
- [Configured .STB file](#) containing business PC menu options

To access a business PC from Station:

1. From any supported Station type on an Experion node, load the previously configured SafeView workspace.
2. Launch Station, and connect to the server using the previously configured .STB file.
3. From the **KVM** menu, choose the business PC you want to connect to and provide credentials if prompted.

The business PC content appears in the pre-configured SafeView position. The Control Panel at the top of the window displays the configured port name.



4. Click **Ctrl + Alt + Del** in the Control Panel to log into the business PC.

5 Administrative tasks

This section outlines administrative tasks you may need to perform on your Raritan KVM implementation, and provides some best practice information to assist with the security of your implementation.

5.1 Upgrading the KVM firmware

To upgrade the Raritan KVM Switch firmware:

1. Download the latest firmware upgrade file from the [Raritan Support site](#), and save it to an Experion node on the Process Control Network.
2. From a browser window on the Experion node, navigate to `https://<KVM IP>/hkc`, where <KVM IP> is the IP address for the KVM Switch as configured earlier in [Configuring the Raritan KVM switch](#).
3. From the KVM login page, enter your administrator credentials.
4. From the KVM Client home page, choose **Maintenance > Firmware Upgrade**.
5. Click **Browse**, and navigate to the directory containing the Firmware Upgrade file.
6. Select the Firmware Upgrade file and click **Open**.
7. Click **Upload**.

The Firmware for your KVM Switch is upgraded. At the time of writing this Tech Note, the Honeywell-certified firmware version is 3.5.0.5.1952.

5.2 Network usage and settings

Typical network traffic impact per session when using KVM to connect to Business computers is shown here:

Usage	Bandwidth*
Basic Operations, including using email software, Office documents etc.	1.1 Mbps
High Traffic usage, including. playing high resolution videos.	4.3 Mbps

*Measured without Bandwidth limit.

NOTE: If you need to comply with NERC CIP guidelines, you will need to monitor the device yourself.

5.2.1 Applying bandwidth limits

You can apply a cap on the bandwidth that a device can use for all sessions through the Raritan Switch.

To set this a bandwidth limit:

1. From the KVM home page, choose **Device Settings > Network**.
2. From the **Bandwidth Limit** list, choose a value as needed.

3. Click **OK** to apply the setting.

NOTE: A low value might result in slower rendering and response when using the Business Computer.

5.3 Troubleshooting

5.3.1 Lag in the content or mouse pointer actions, or incorrect content colors.

Resolution: Click **Sync Video** in the KVM Client Control Panel to synchronize the SafeView display and the content in the remote display.