Publish a browser-in-browser kiosk scenario in an RDS session/application in Parallels Secure Workspace

- Parallels Secure Workspace

Resolution

This scenario is especially useful in cases where publishing a reverse proxied web application is for some reason not sufficient. (e.g. the application doesn't properly support reverse proxying, difficulties with authentication, ...).

Benefits

- Enjoy the benefits of the browser's kiosk mode.
- Not the entire browser is visible inside the Parallels Secure Workspace application session. For example, the address bar etc. can be hidden so it does not take unnecessary space on the screen.
- Advanced authentication methods are possible.

Steps

1. On a Microsoft Windows RDS infrastructure:
    1. Publish the browser as a RemoteApp.
    2. In the RemoteApp properties (right-click in the Microsoft Windows RDS configuration on the RemoteApp> Edit Properties), go to the Parameters and enter the URL of your intranet site as a fixed command-line parameter (see screenshot).
        - ◊ Kiosk mode command for Internet Explorer:
          `-k "your.intranet.local"`
        - ◊ Google Chrome, Microsoft Edge, Mozilla Firefox:
          `--kiosk "your.intranet.local"`
        - ◊ When using Google Chrome: use the parameters below instead to keep the ability to move/close the browser window.
          `--new-window --app=your.intranet.local`
2. In Parallels Secure Workspace, publish the browser as a Remote Application.

Authentication / automatic logon

Configuring Google Chrome and Mozilla Firefox for Windows Integrated Authentication

Windows Integrated Authentication allows a user's Active Directory credentials to pass through their browser to a web server.

Windows Integrated Authentication is enabled by default for Internet Explorer, but not for Mozilla Firefox.

Users who use non-Microsoft browsers may receive a pop-up box to enter their Active Directory credentials before continuing to the website. Note that the most recent Google Chrome version just takes the same settings as for Internet Explorer.

This adds additional steps and complexity for users who are using web-based applications. In an effort to make this process as easy as possible for end-users, many IT administrators enable Windows Integrated Authentication for the third-party browsers.

Configuring Delegated Security for Mozilla Firefox

To configure Mozilla Firefox to use Windows Integrated Authentication:

1. Open Mozilla Firefox
2. In the address bar, type `about:config`
3. A security warning will be shown. To continue, click Accept the Risk and Continue. Use the search box to search for the following settings. Once you have located each setting, update the value to the following:

Setting	Value
network.negotiate-auth.delegation-uris	sampleserver.yourdomain.com
network.automatic-ntlm-auth.trusted-uris	sampleserver.yourdomain.com
network.automatic-ntlm-auth.allow-proxies	True
network.negotiate-auth.allow-proxies	True

Note: sampleserver.yourdomain.com points to the FQDN of the server for which authentication will be enabled.

Configuring Google Chrome, Microsoft Edge, Microsoft Internet Explorer for automatic logon using Group Policy

1. Open the **Group Policy Management Console**, and then either create a **new Group Policy Object (GPO)** or **edit** an existing GPO.
2. Expand **Computer Configuration > Policies > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Click/open the Security Page** folder.
3. In the **details** pane, double-click **Site to Zone Assignment List.**
4. In the **Site to Zone Assignment List** Properties dialog box, click **Enabled**.
5. Next to Enter the zone assignments here, click **Show**.
6. In the Show Contents dialog box, type the **URL** of your website (for example, https://yourorg.contoso.com) in the Value name box/column.
7. Type for example **1 (indicating the local intranet zone)** in the Value box/column, and then click OK. Other options are listed at the end.
8. In the **Site to Zone Assignment List** dialog box, click **[OK]**.
9. In the **Group Policy Management** Editor, enter the appropriate zone folder (for example, "Intranet Zone").
10. In the **details** pane, double-click **Logon** options.
11. In the **Logon** options **Properties** dialog box, click Enabled.
12. In the **Logon** options list, click **Automatic logon only in Intranet zone**, and then click **OK**.
13. Close the **Group Policy Management** Editor.

Note: it's possible to use a different zone, such as "Trusted Sites" zone.
Just make sure the "Automatic logon" option is set for the zone you choose.

(1) Intranet zone
(2) Trusted Sites zone
(3) Internet zone
(4) Restricted Sites zone.