BeyondTrust

Privileged Identity
App Launcher and Session Recording

TC:1/6/2021

Table of Contents

Application Launcher and Session Recording

The goal of application launching is to put a user into a privileged session and limit their access to a specific application and a single connection. The BeyondTrust Privileged Identity (PI) application launcher is designed to launch a wide range of programs and processes. From the web application, you can click a link and connect to a target endpoint through a jump server using credentials from BeyondTrust PI. Or, you can use the BeyondTrust PI API. Additionally, the application launcher provides free session recording to capture the entire session in a video, which can be played back via a streaming media server.

This guide explains how to install the BeyondTrust Privileged Identity application launcher and session recording software.

Application Launcher Installation and Deployment Considerations

Review the tasks required to install the application launcher and session recording software for Privileged Identity.

Installation Tasks

1. Install and register the Privileged Identity management console, the web application, and web service.
2. Make note of the web service URI. It is required for the application launcher and session recording to work properly.
3. Understand the product requirements prior to installation.
4. Install the application launcher and (optionally) the session recording software.
5. Install streaming media services for IIS.
6. Configure application launching settings via the management console.

Plan Your Session Recording Installation

The application launching capability of Privileged Identity is a licensed feature, which requires a jump server. An application launcher server needs to be a Windows Remote Desktop Services (RDS) machine which can proxy connections to specific target systems.

The general configuration for application launcher includes:

- Installation of Privileged Identity
- Jump server or multiple jump servers to launch applications

> ***Note:*** *We recommend jump servers be hosted separately from your main BeyondTrust Privileged Identity instance.*

When session recording is enabled, the following should be considered:

- **Recording**: The session recording component on the jump server records the session and copies the resulting file(s) for video transcoding to the machine/folder, which functions as the video transcoder.
- **Transcoding**: The video transcoding service compresses the raw video file and processes it for streaming.

> ***Note:*** *We do not recommend installing the transcoding component on your jump server due to potential storage and CPU usage issues and instead recommend installing the component on a separate machine. However, a single server configuration is supported.*

- **Storage**: The transcoded file is moved to permanent storage. This could be the file system of the transcoder or another system providing access from the final files to the streaming media services machine.
- **Streaming** - The media server component streams the video files for viewing on demand and requires access to the storage where the video files are located. This machine may be a shared machine or a separate machine.

High Availability Suggestions

High Availability (HA) is achieved by deploying multiple instances and configuring load balancing. A few examples and suggestions of how HA can be achieved are provided below:

- **Jump server**: The application launcher relies on Microsoft Remote Desktop Services (RDS), and RDS uses Network Load Balancing (NLB) to achieve high availability.
- **Transcoding**: If transcoding occurs on another machine separate from the jump server, you can deploy multiple transcoders and point to where the recorder will place the raw, non-transcoded files. If transcoding occurs on your jump server and the jump server is already configured as part of an NLB cluster, you can install the transcoder on each host.
- **Storage**: To retain multiple live copies of recorded sessions, you can use a replicated storage solution like a Distributed File System (DFS) to replicate the data.
- **Streaming**: To enable HA for streaming, you can maintain multiple instances of the media server configured as an NLB cluster and point to the same shared storage.

Note: *The recorded video files are located in the file system of the host operating machine. A simple backup strategy may be beneficial and may make the deployment process easier.*

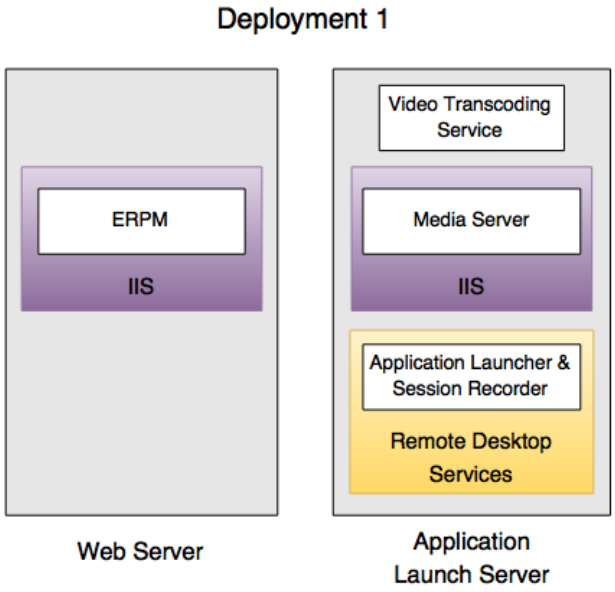
Potential Deployment Strategies

There are several ways to deploy the application launcher and the session recording software. If using the session recording component, your deployment strategy may be more complex.

Here are three potential deployment scenarios.

Deployment 1

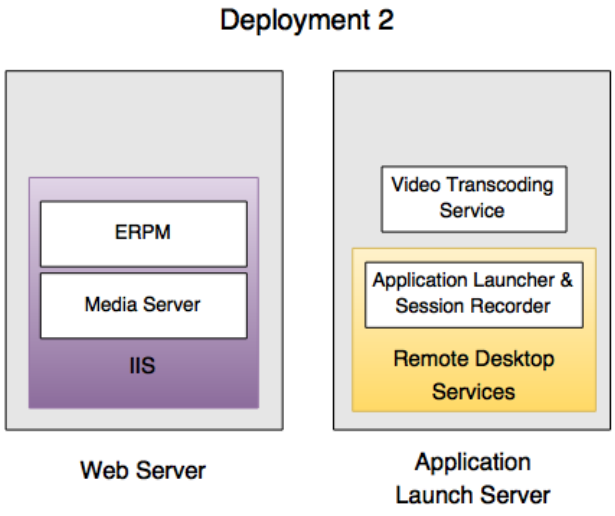
Place the recording, transcoding, and streaming components on the jump server.



Deployment 2

Place the recording and transcoding components on the jump server, and the streaming component on the web server. If the CPU on the jump server is powerful enough and can quickly process raw video for streaming, this deployment model may be ideal.

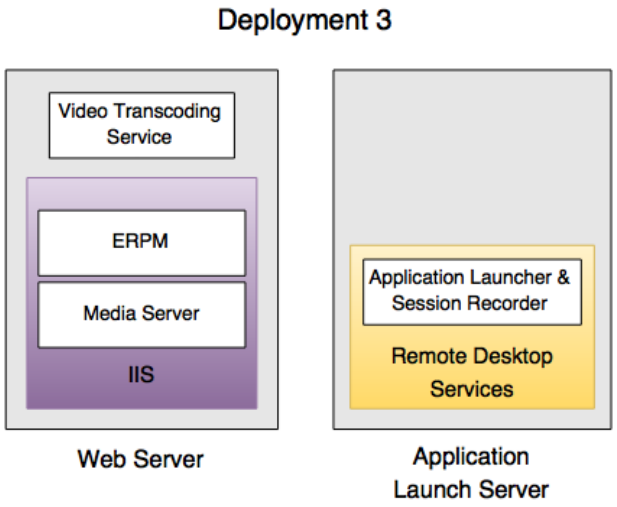
> ***Note:*** *This deployment model does not require IIS to be configured on the jump server.*



Deployment 3

Place the recording component on the jump server, and place the transcoding and streaming components on the web server. This model is recommended.

> ***Note:*** *Before deployment, make sure your web server is appropriately sized to handle the output from the video transcoding service.*



Application Launcher and Session Recording Prerequisites

This section outlines the installation prerequisites for the Privileged Identity application launcher and session recording software. Based on your starting host system configuration, your actual installation experience may vary.

Recommended Knowledge

While BeyondTrust provides documentation and support to install and configure the application launcher and session recording software for Privileged Identity, product administrators should have experience in the following areas:

- Knowledge of the Windows environment
- IIS web server technologies
- Network administration
- System administration

Note: *Privileged Identity component host servers should be patched, secured, and properly configured in conjunction with your corporate patching strategy to ensure the password store system is not compromised.*

Application Launcher and Session Recording Requirements

Application Launcher Platform Requirements

A Windows Server operating system is required for any installation of the application launcher. The solution is fully supported on a physical server or a virtual machine, regardless of the virtual host platform. All service pack levels and editions of the supported operating systems are supported, except where specifically noted. BeyondTrust recommends using the most current version of Windows Server.

Supported Windows versions:

- Windows Server 2016
- Windows Server 2012 R2

Application Launcher Hardware and Software Requirements

- Web Service installed and configured with a valid and trusted SSL certificate
- Microsoft .NET Framework 4.5.2+
- Microsoft Remote Desktop Services (RDS) with proper licensing
- RAM and CPU appropriate for the number of users and applications using application launcher

IMPORTANT!

High availability should be employed whenever possible. All components of Privileged Identity support a high availability configuration.

Session Recording Platform Requirements

A Windows Server operating system is required for any installation of the session recording component. The solution is fully supported on a physical server or a virtual machine, regardless of the virtual host platform. All service pack levels and editions are of supported operating systems are supported, except where specifically noted. BeyondTrust recommends using the most current version of Windows Server.

Supported Windows versions:

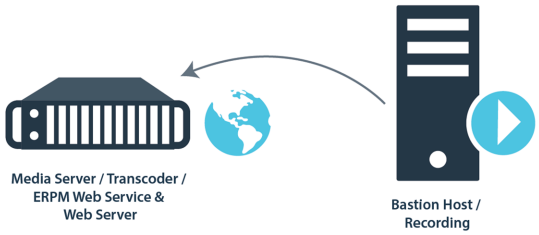
- Windows Server 2016
- Windows Server 2012 R2

Session Recording Hardware and Software Requirements

- Microsoft .NET Framework 4.5.2+
- Microsoft .NET Framework 3.5 SP1
- Multi-core CPUs
- 2 GB+ RAM

Minimum Requirements for Bastion Hosts

The following requirements are for launching applications on a bastion host.



> ***Note:*** *The bastion host can function as the video transcoder and media server; however, this will impact the performance of the host during video transcoding.*

- **Bastion host**: RDS host
  - 2 GB RAM
  - 2+ CPU cores;
  - .NET Framework 4.5.2+

> For more information about RDS sizing, please see the Microsoft Help Center at docs.microsoft.com.

- **Session Recorder / Media Server**
  - 2 GB RAM
  - 2+ CPU cores
  - NET Framework 4.5.2+
  - IIS
  - Microsoft Media Services (included in download)

> ***Note:*** *The amount of free disk space required depends on the number of recordings being stored.*

Recommended Hardware for Deploying Application Launcher with Session Recording

If you wish to deploy application launcher with session recording, BeyondTrust recommends the following hardware:

- **Bastion host**: RDS host
  - 6 GB+ RAM
  - 4+ CPU cores (not including hyper-threading)
  - .NET Framework 4.5.2+
  - Multiple RDS hosts configured as an RDS farm
- **Session Recorder / Media Server**
  - 4 GB+ RAM
  - 4+ CPU cores (not including hyper-threading)
  - .NET Framework 4.5.2+
  - Microsoft Media Services (included in download)
  - Storage for recorded videos (can be on a distributed file system (DFS) share)

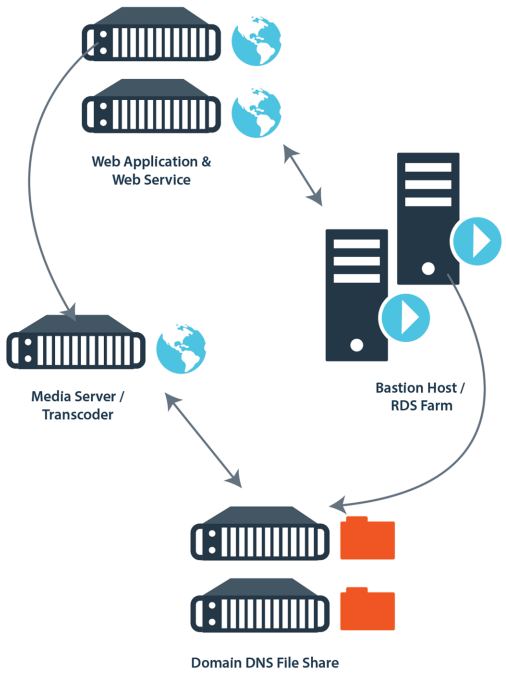
Example

In the diagram shown, an Active Directory-based Distributed File System (DFS) is depicted as the storage for raw and converted session recording files. DFS is not a requirement, but it is recommended in order to add online redundancy for the storage of the recorded sessions.

In this scenario, the bastion host records raw sessions and copies them to the DFS share. The media server transcodes the files from the DFS share, writes the converted files back to the DFS share, and deletes the original raw files.

If a DFS share is not used, the bastion host moves the raw files to the media server, performs video transcoding services, and stores the files locally.

In either case, the media server provides access to the recorded sessions via IIS and Microsoft Media Services.



Media Server Requirements

Platform Requirements

A Windows Server operating system is required for any installation of streaming media services. The solution is fully supported on a physical server or a virtual machine, regardless of the virtual host platform. All service pack levels and editions of supported operating systems are supported, except where specifically noted. BeyondTrust recommends using the most current version of Windows Server.

Supported Windows versions:

- Windows Server 2016
- Windows Server 2012 R2

Hardware and Software Requirements

- Internet Information Services (IIS)
- 2 GB+ RAM

Service Account Requirements for App Launcher

Multiple service accounts may be used during this process. If one service account is used for more than one component, combine the permissions required for the account.

Application Launcher Service Accounts

The application launcher uses a single account to log into the jump server on behalf of the user and to launch the application. This account should be a domain-joined account and can be managed by Privileged Identity, provided it is not also running deferred or zone processing services. The account has no explicit requirements other than it must be allowed to RDP to the jump server host. This typically only requires membership in the **Remote Desktop Users** group on the jump server.

Other considerations for this service account are:

- If the web service is leveraging Integrated Windows Authentication, this account must be able to connect to the web service without being prompted for a username and password.
- When connecting to the web service with the account, no SSL trust issues can be encountered.
- Depending on the application being launched, the account may require additional permissions on the jump server. For example, if the application being launched requires administrative privileges to run on the jump server, this service account must have administrative group membership on the jump server.

Session Recording Service Accounts

Session recording service account requirements vary based on deployment.

All roles on same server

- If session recording, transcoding, and media service roles are installed on the jump server, it is sufficient to configure the application to use **Local System** since no network access is required.

Recorder role on jump server, media server, and transcoder services on a separate host

- The jump server login account must have network access and must be able to modify permissions to the **Source** share on the transcoder host.
- On the jump server, the session recording service account should be configured as **Network Service**.
- Through the **Windows services snap-in**, session recording services may be disabled post-install.
- The transcoding host service account may be configured as **Local System** or a named account. If running as a named account, this account must be granted **Logon as a service**. Network access is required from the transcoder host for the video files, as the media server is on the same host.
- The transcoding host service account must be granted **Modify** access to the **Source**, **Working**, and **SessionRecording** directories on the transcoder host. The actual paths are defined during installation.

Recorder role on jump server, transcoder on a separate host, and media server on a separate host with local storage

- The jump server login account must have network access and must be able to modify permissions to the **Source** share on the transcoder host.
- On the jump server, the session recording service account should be configured as **Network Service**.
- Through the **Windows services snap-in**, session recording services may be disabled post-install.
- Transcoding host service account must be configured as a named account.
- Transcoding host service account must be granted **Logon as a service**.

- Transcoding host service account must be granted modify access to the **Source** and **Working** directory on the transcoder host. The actual paths are defined during installation.
- Transcoding host service account must be granted **Write** access to the **SessionRecording** share on the media server host.

Recorder role on jump server, transcoder on separate host, and media server on separate host with remote storage

- The jump server login account must have network access and must be able to modify permissions to the **Source** share on the transcoder host.
- On the jump server, the session recording service account should be configured as **Network Service**.
- Through the Windows services snap-in, session recording services may be disabled post-install.
- Transcoding host service account must be configured as a named account.
- Transcoding host service account account must be granted **Logon as a service**.
- Transcoding host service account must be granted **Modify** access to the **Source** and **Working** directory on the transcoder host. The actual paths are defined during installation.
- Transcoding host service account must be granted **Write** access to the **SessionRecording** share on the storage system connected to the media server host.
- If the storage system for the media server is a remote server, configure the **SessionRecording** virtual directory in IIS with network credentials valid on the remote storage system, and grant **Read** permissions to that directory for the account.

Note: *It is possible to configure every component to use the same service account. Because there are different access requirements, using a single service account for all components is fully supported and recommended. However, this can make the configuration and maintenance unnecessarily complex.*

Port Requirements for App Launcher

Application launcher and session recording software make use of a small number of ports. Actual port usage varies based on your specific configurations.

Note: *The following ports are the standard ports for common protocols. These ports may have been changed on the target system. It is the responsibility of the administrator to determine if any of the target ports have been changed and reflect changed ports when password change jobs or account discovery jobs are performed.*

Ports	Direction	Use
53	TCP/UDP, outbound, DNS	Used for name resolution to target hosts.
88	TCP/UDP, outbound, Kerberos	When Kerberos authentication is configured,used by the jump server to authenticate users.
443	TCP, outbound, HTTPS	Used by the application launcher and web service to communicate with the Privileged Identity web service.
445	TCP, outbound, SMB	When hosted across multiple servicers, used by session recording components to copy recorded files to other session recording component hosts.
464	TCP/UDP, outbound, Kerberos	When Kerberos authentication is configured, used by the jump server to authenticate users.
3389	TCP/UDP, inbound, RDP	Used by the end user to connect to remote applications installed on the jump server.
389/636	TCP, outbound, LDAP/LDAPS	During the login of the application launcher, used by the jump server to communicate with Active Directory.

Note: *Applications will require ports specific to their function. They are not defined by Privileged Identity.*

Note: *If either the web service or the web app is on a non-default port, you must configure the firewall to allow communication over that port.*

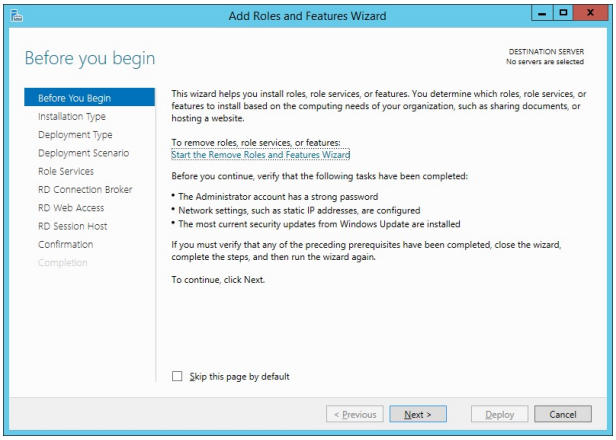
Application Launcher and Session Recording Installation

Install Remote Desktop Services

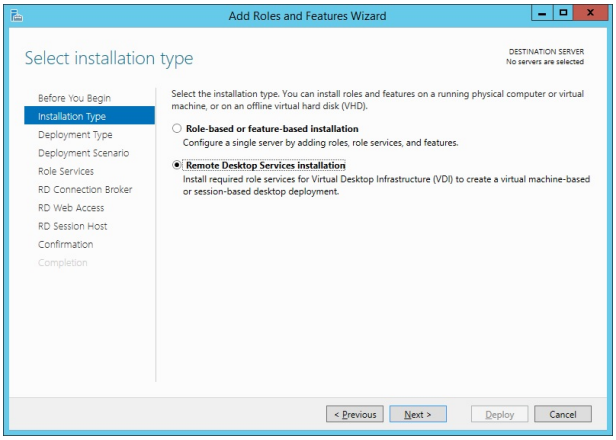
This section explains how to install Microsoft Remote Desktop Services (RDS) on a Windows server host. If multiple jump servers are used, Privileged Identity does not require them all to run on the same operating system. However, they all need to use Windows Server 2012 R2+. We recommend using the most current version of Windows Server.

Privileged Identity uses a single login account to connect to the jump server. This account is used to launch applications, and it does not have to be an administrator account unless a specific application requires administrative rights to run. If the account is not configured as an administrator, it must be granted the right to log in via RDS. This can be granted by adding the account to the **Remote Desktop Users** local group.

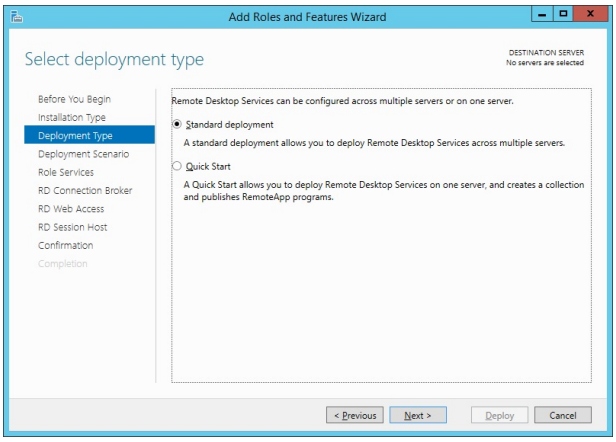
1. Open **Server Manager**. Select **Add Roles and Features**.
2. Click **Next** on the **Before You Begin** page.



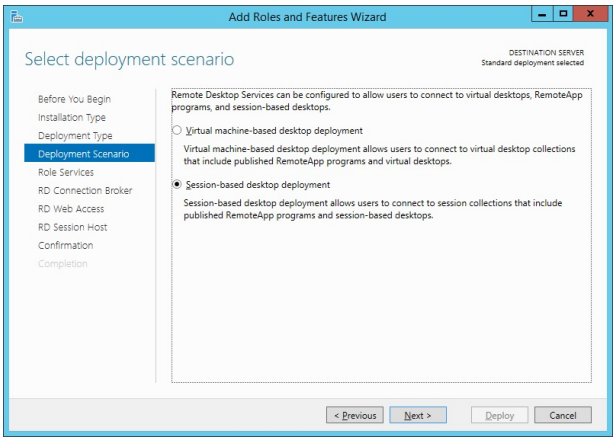
3. On the **Select installation type** page, select **Remote Desktop Services** installation. Click **Next**.



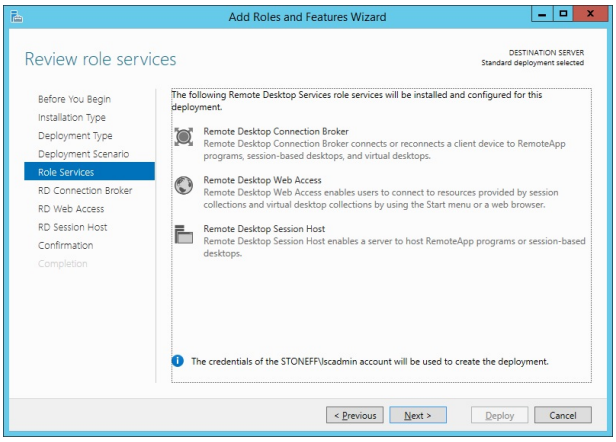
4. On the **Select deployment type** page, choose a deployment type and click **Next**. Selecting **Standard deployment** requires the administrator to configure a collection post-RDS installation. The **Quick Start** method is faster and automatically creates a collection. However, it also adds and publishes additional applications that are not needed and does not provide configuration options.



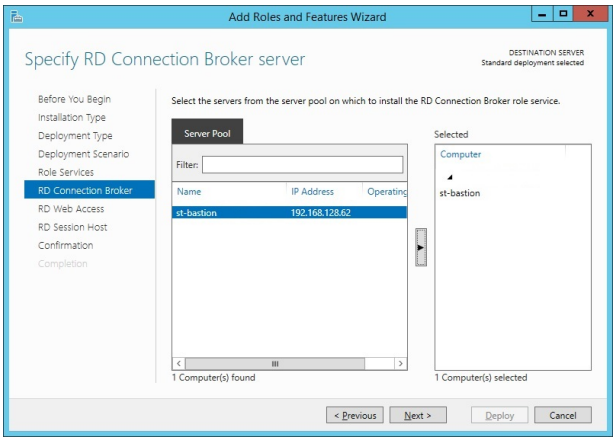
5. On the **Select deployment scenario** page, select **Session-based desktop deployment**. Click **Next**.



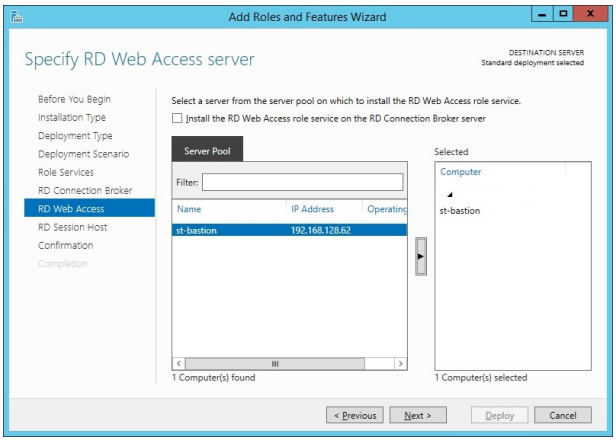
6. Click **Next** on the **Role Services** page.



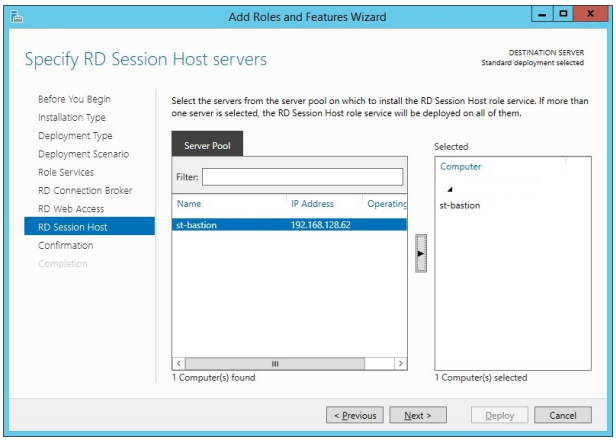
7. On the **Specify RD Connection Broker server** page, select the server from the **Server Pool** field. Add it to the **Selected** computer field by clicking the arrow between the two fields.
8. Click **Next**.



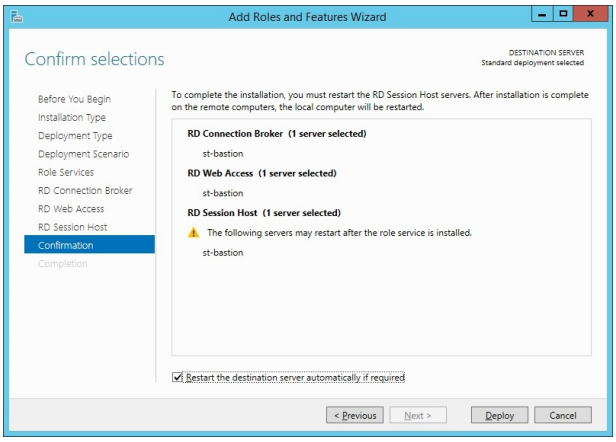
9. On the **Specify RD Web Access server** page, select the server from the **Server Pool** field. Add it to the **Selected** computer field.



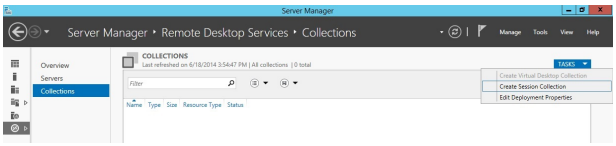
10. Click **Next**.



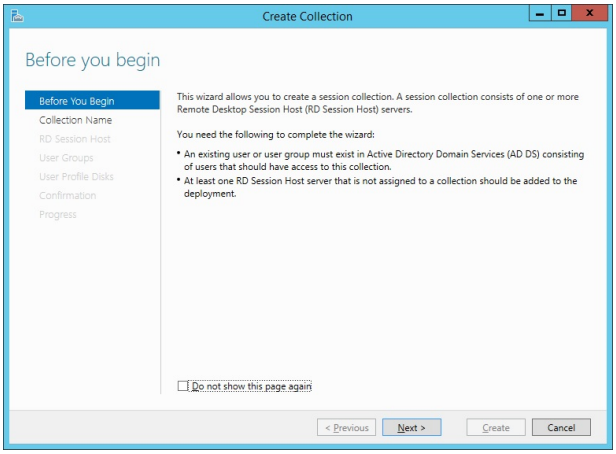
11. On the **Confirm selections** page, click **Deploy**. If required, restart the host.



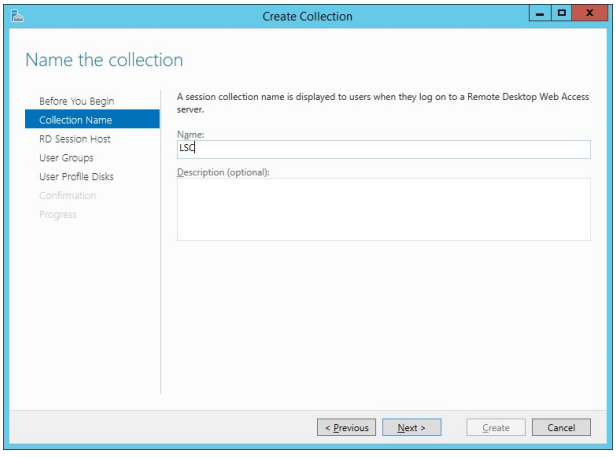
12. After restarting, open **Server Manager > Remote Desktop Services**. Click **Collections**.
13. At the top right corner, select **Tasks > Create Session Collection**.



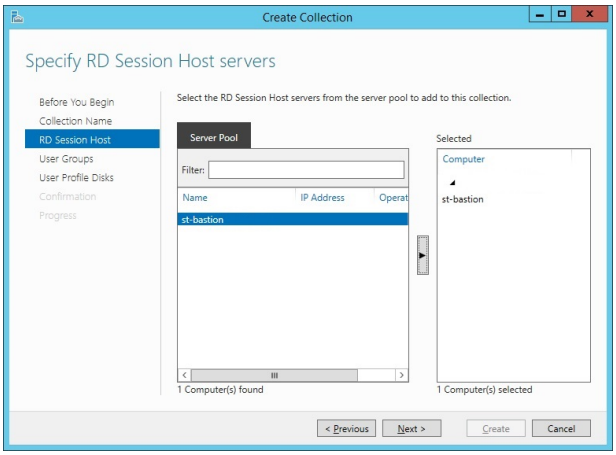
14. On the **Before you begin** page, click **Next**.



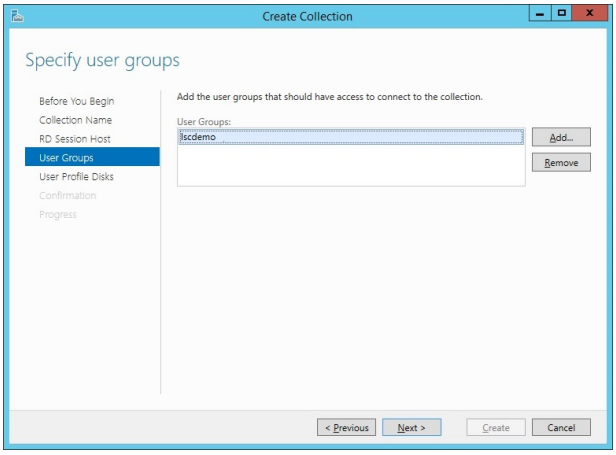
15. On the **Name the collection** page, supply a friendly name for the collection and click **Next**. The collection name should be 16 characters or less (due to Microsoft design limitations).



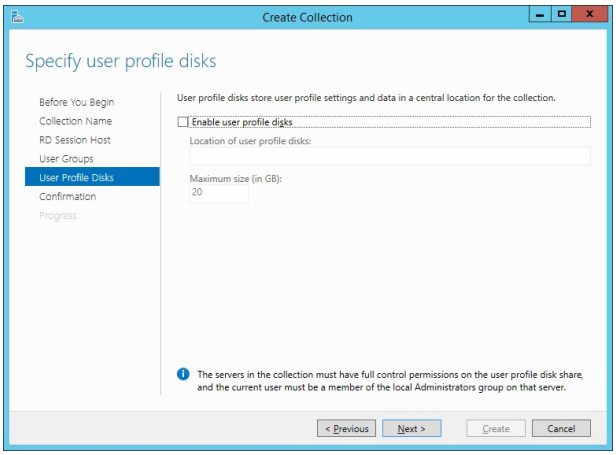
16. On the **Specify RD Session Host server** page, select the server from the **Server Pool** field. Add it to the **Selected > Computer** field. Click **Next**.



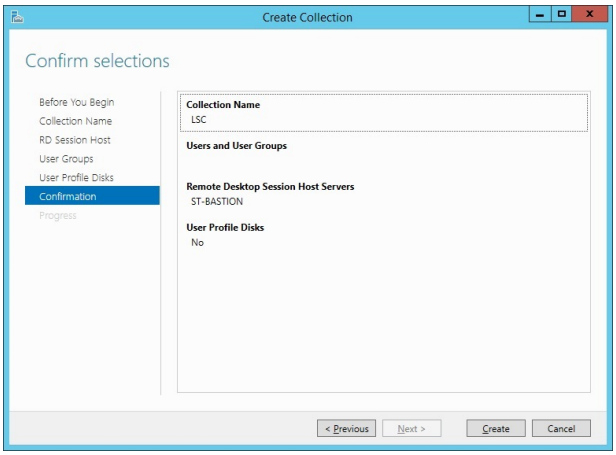
17. Select a proxy account to connect the jump server to prior to launching the selected application. This account either needs to be added to a group that can RDP to the target jump server to launch subsequent applications, or the account should be added directly as a user that can connect to the RDP session host server.
18. Click **Next**.



19. On the **Specify user profile disks** page, click **Next**.



20. On the **Confirm selections** page, click **Create**. An empty collection is created.



Install Microsoft Desktop Experience

IMPORTANT!

If you enable session recording, you do not need to install the Desktop Experience feature.

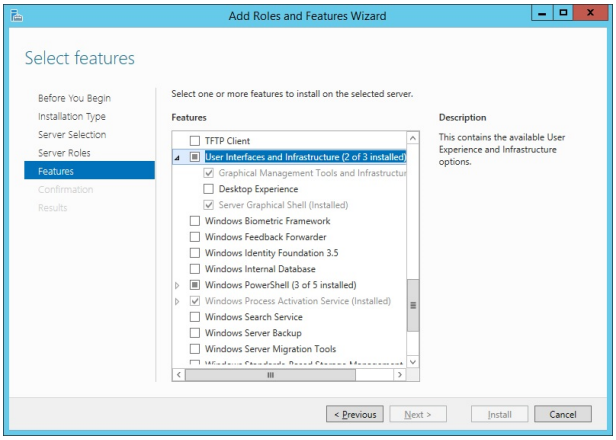
Microsoft Desktop Experience is included with Windows Server 2012 R2.

If you install the video transcoding service, Application Launcher, and session recording components on separate systems, install Desktop Experience on the jump server and the system running the video transcoder. You do not need to install Desktop Experience on the streaming media server.

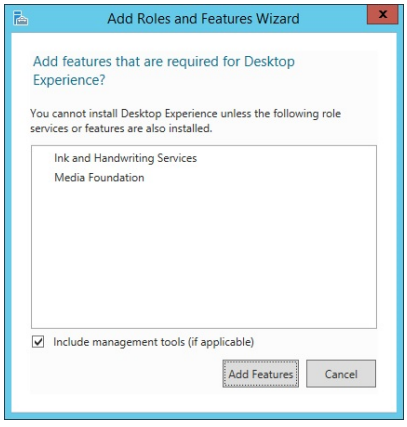
For more information about Microsoft Desktop Experience, please see Desktop Experience Overview at https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn609826(v=ws.11).

Install Desktop Experience

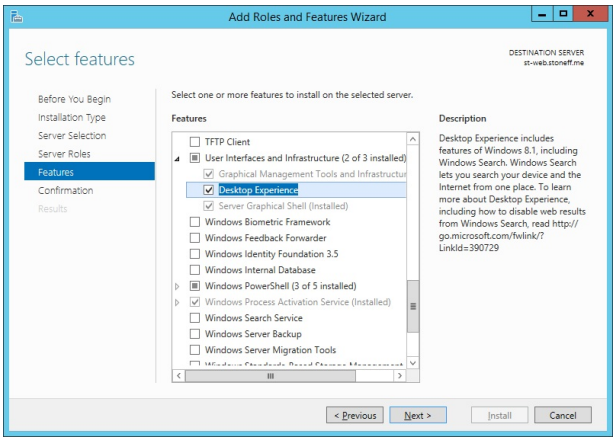
1. To add Desktop Experience, open **Server Manager** and select **Add Features**.
2. On the **Features** page, expand **User Interfaces and Infrastructure**. Select **Desktop Experience**.



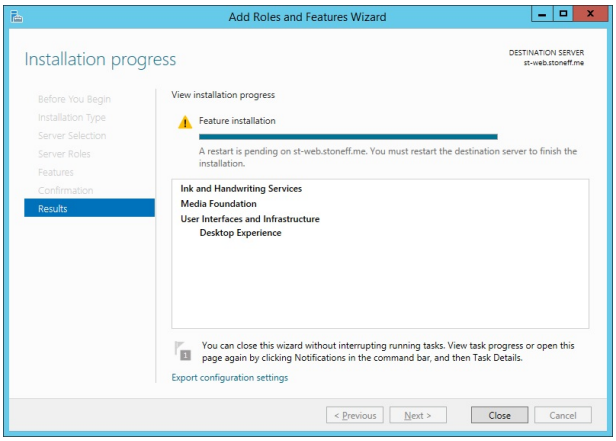
3. If prompted for additional components, click **Add Features**.



4. Add any other requirements that other applications launched from this system may require, such as .NET Framework 4.x+ Click **Next**.

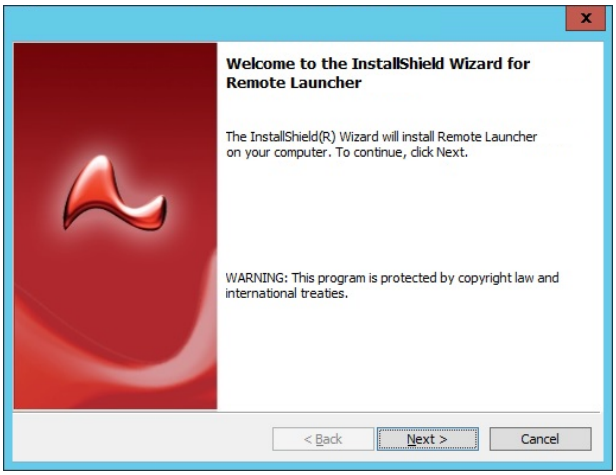


5. Continue through to the end of the wizard. Click **Close** and restart the host.

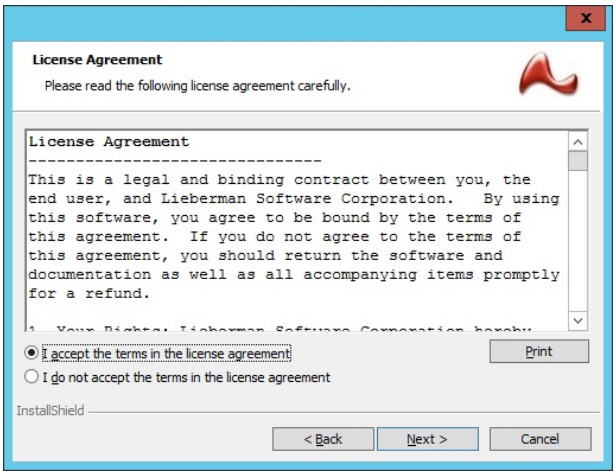


Install the Application Launcher and Session Recording Software

1. To begin installation, open the **SupplementalInstallers** sub-folder from the installation directory, **%ProgramFiles (x86)\Lieberman\Roulette**.
2. Copy **ERPMRemoteLauncherInstaller.exe** to the machine functioning as the transcoder, and launch the installer.
3. Click **Next** on the **Welcome** page.

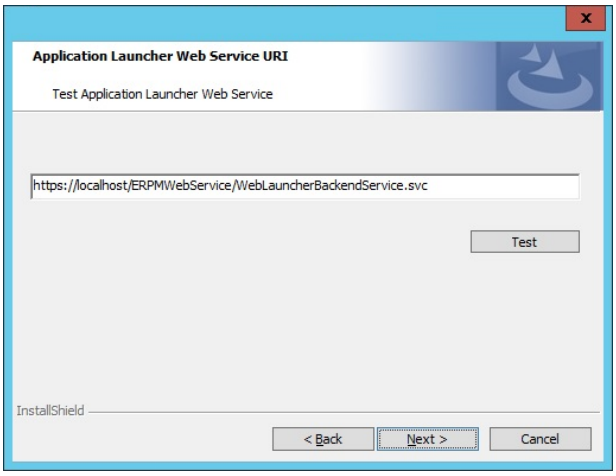


4. Read and accept the license agreement. Click **Next**.



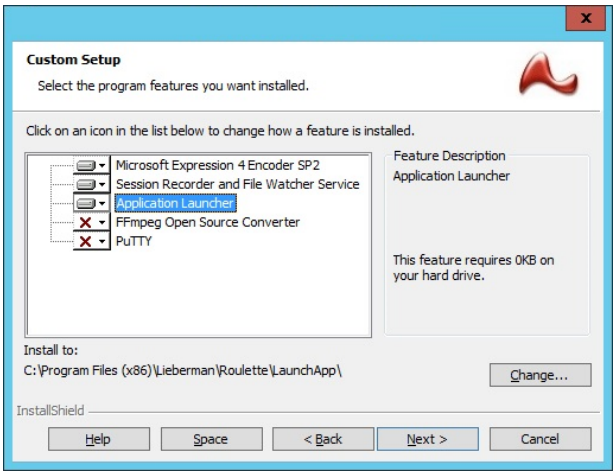
5. Enter the full SSL-secured URL to the web service. Web Services are installed separately on the web application server. The application launcher web service is installed with the standard **ERPMWebService** installer package, **https://server.example/ERPMWebService/WebLauncherBackEndService.svc**.

6. Click **Test** to validate the URL. All certificate issues must be corrected before installation can succeed. If the web page does not appear at all, validate the URL and try again, or install **Web Services**.
7. If no issues or errors are encountered, click **Next**.



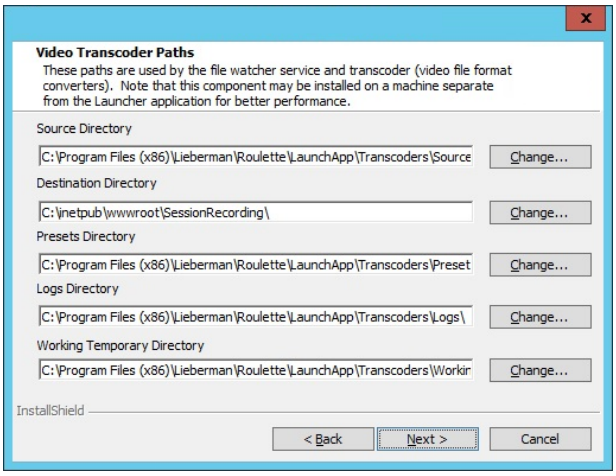
8. **If session recording WILL NOT be enabled, select to install:**
   - Application Launcher

   For the Application Launch Server host, if session recording WILL BE enabled, select to install:
   - Microsoft Expression 4 Encoder SP2
   - Session Recorder and File Watcher Service
   - Application Launcher
9. Select the installation directory. Click **Next**.

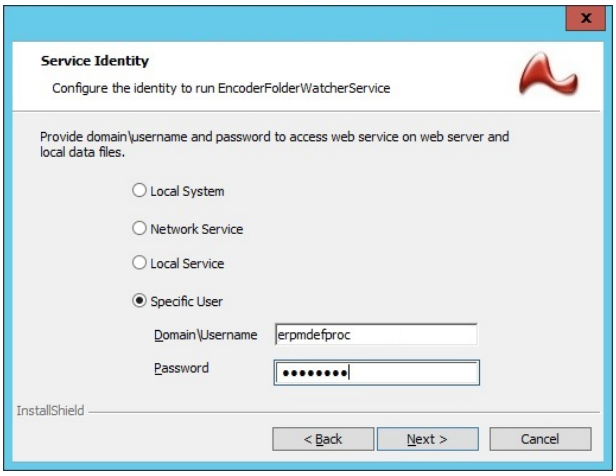


> ***Note:*** *If session recording components are not enabled, clicking* ***Next*** *installs the application launcher software and completes the installation.*

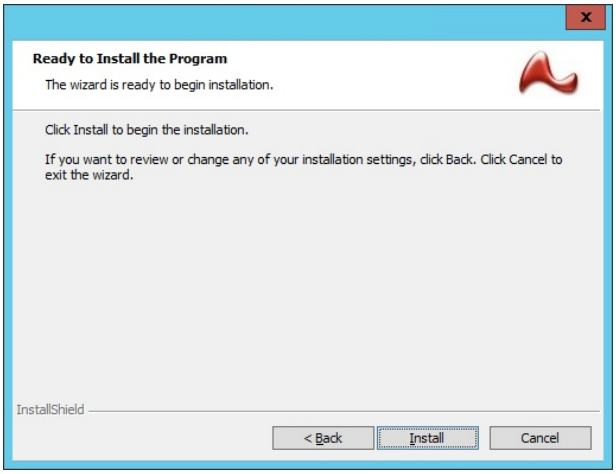
10. If session recording components are being installed, the next dialog configures the session recording paths.
    - The destination directory is where completed video files are placed after being transcoded. If this machine is functioning as the transcoder host as well and the media server is a separate machine, specify the network path to the **SessionRecording** share on the media server host.
11. Click **Next**.



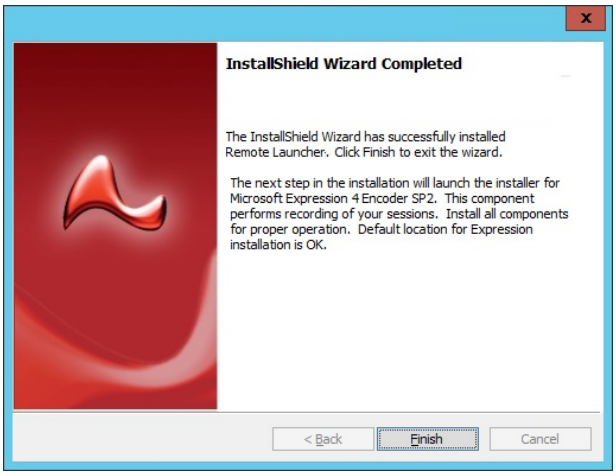
12. On the jump server host, select to run the service identity as either a **Specific User**, **Network Service**, or **Local System**.



    - **Local System** offers the benefit of already having proper access and no password management requirements. If the transcoder is running on a separate system and local system is used, the computer account of the jump server must be granted **Modify** access to the source directory on the transcoder host.
    - **Network Service** provides fewer rights than local system and offers the benefit of already having proper access and no password management requirements. If the transcoder is running on a separate system and network service is used, the computer account of the jump server must be granted **Modify** access to the **Source** directory on the transcoder host. **NT Authority\Network Service** must also be granted **Modify** access to the **Session Recording** directory.
    - **Specific User** offers the path of least privilege but requires configuring NTFS permissions on the **Source** directory. When the transcoder is on a separate system, running as a specific user is recommended for running the **File Watcher** service on the jump server.
13. Click **Next**.
14. Click **Install**.



15. Click **Finish** to complete the first part of the installation.



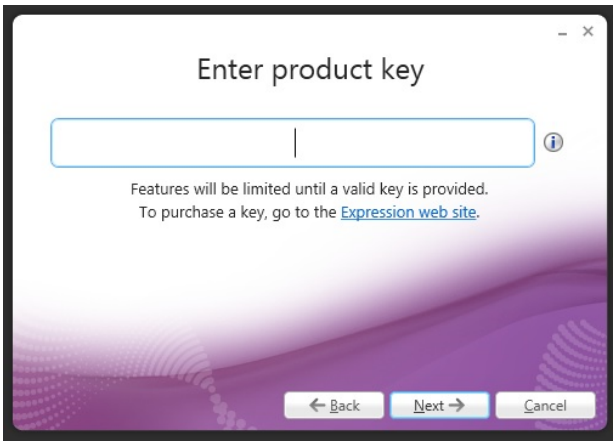
IMPORTANT!

If session recording components were not selected during the installation process, the installation ends. If any of the session recording components were selected, a separate installation for the Microsoft Expressions recorder is initiated.

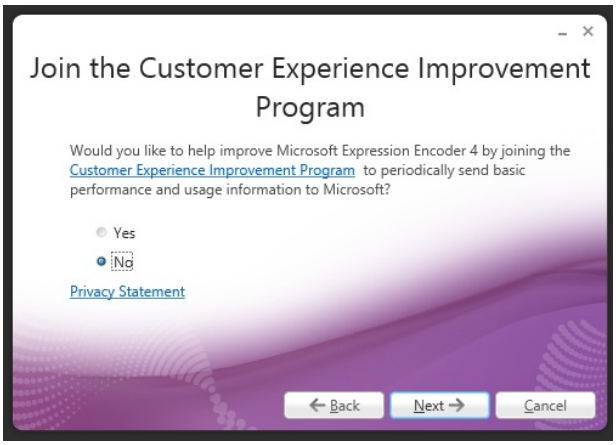
Install Microsoft Expressions Recorder

1. Accept the license agreement for the Microsoft Expressions recorder.

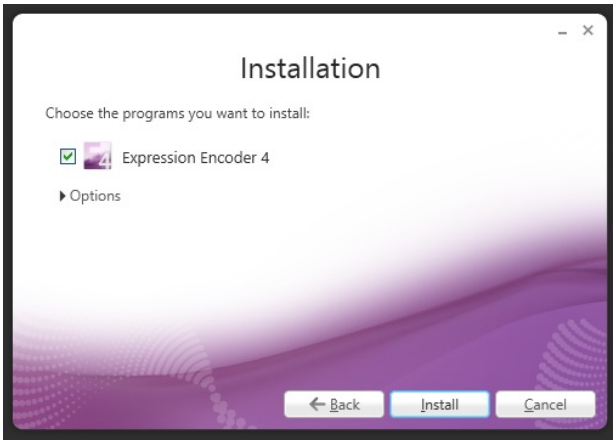
2. Click **Next** on the **Enter product key** page. No product key needs to be entered.



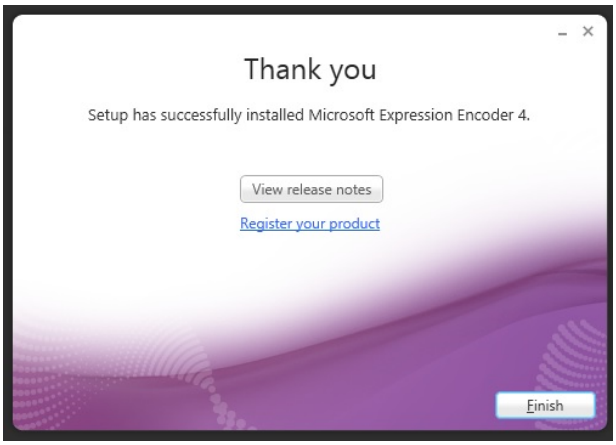
3. Choose if you would like to join the **Microsoft Customer Experience Improvement Program**. Click **Next**.



4. Select to install **Expression Encoder 4**. Click **Install**.



5. Click **Finish** to complete the installation.



6. Other tasks are performed that are not not visible in the installer, including:
    - A **[Domain] Local** security group is created called **WriteRecordingGroup**. If the installation is taking place on a domain controller, the group is created in the **Users** container. This group may be safely deleted from the jump server if also functioning as the transcoder host.
    - The **Domain Admins** group is added to this **WriteRecordingGroup**.
    - The installer creates and shares the following directory: **%inetpub%\wwwroot\SessionRecording** as **SessionRecording**. This directory is used to copy compiled session recordings from the jump server to the transcoder host. This scenario applies if using the FFMPeg video recorder rather than the Expressions recorder. This share directory will be required when configuring the jump server for app launching with session recording. If the transcoder and jump server are the same system, this share can be safely deleted.
    - The installer creates and shares the following directory: `%ProgramFiles(x86)%\Lieberman\Roulette\LaunchApp\Transcoders\Source` as **Source**. This directory is used by the jump server to copy raw session recording files to the transcoder host. This scenario would apply if using the Expressions 4 recording software. This share directory is required when configuring the jump server for app launching with session recording. If the transcoder and jump server are the same system, this share can be safely deleted.
    - Each of the shared directory's share permissions are set to allow full control of the **WriteRecordingGroup**. Minimum permission required is **Change**.

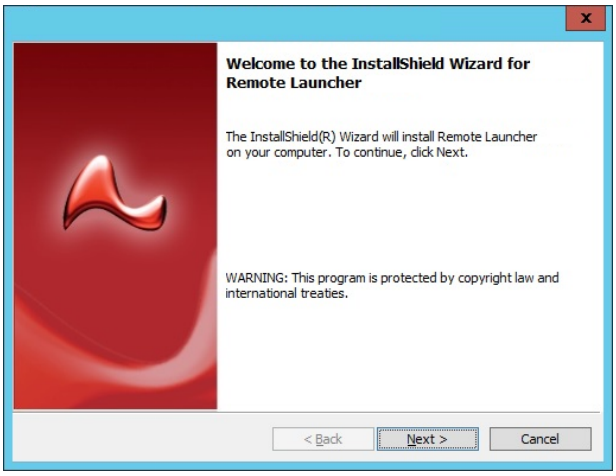
Install the Session Recording Software on the Transcoder Host

IMPORTANT!

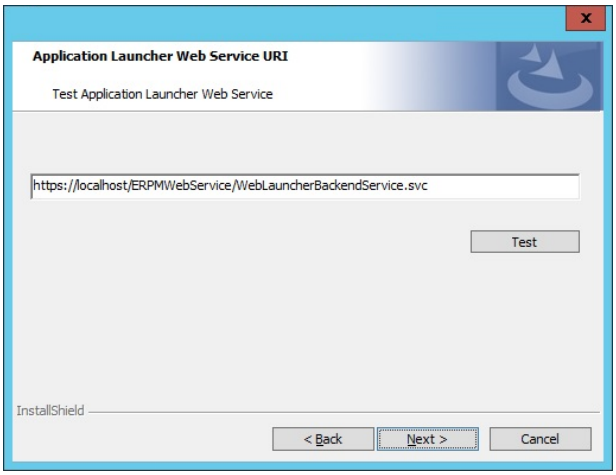
If you are not installing and using the session recording software, skip this step.

1. To begin installing the session recording software, open the **SupplementalInstallers** sub-folder from the installation directory, **"%ProgramFiles (x86)\Lieberman\Roulette"**.
2. Copy **ERPMRemoteLauncherInstaller.exe** to the machine functioning as the transcoder. Launch the installer.
3. Click **Next** on the **Welcome** page.
4. Read and accept the license agreement to continue installation. Click **Next**.
5. Enter the full SSL-secured URL to the web service. Web Services are installed separately. The application launcher web service is installed with the standard ERPMWebService installer package. The URL is

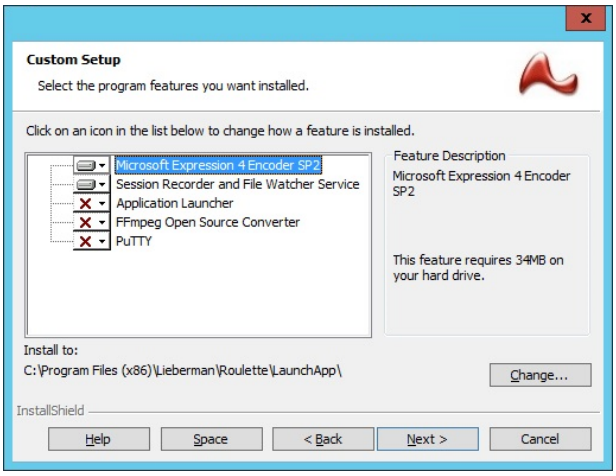
   https://server.example/ERPMWebService/WebLauncherBackEndService.svc.



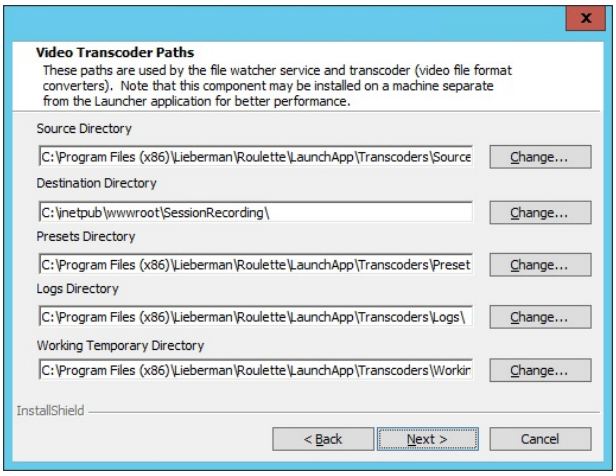
6. Click **Test** to validate the URL. Any certificate issues must be corrected before installation will succeed. If the web page does not appear at all, validate the URL and try again, or install web services.
7. If the page tests without issue or errors, click **Next**.



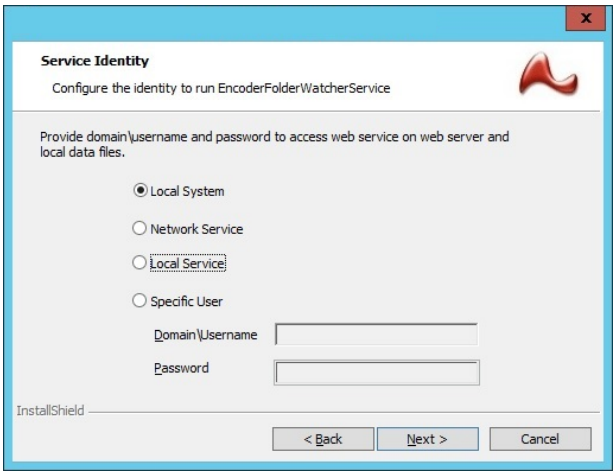
8. For the transcoder host, select to install:
    - Microsoft Expression 4 Encoder SP2
    - Session Recorder and File Watcher Service
9. Select the installation directory. Click **Next**.



10. Specify the network path to the **SessionRecording** share on the media server host. If this system will server as both the transcoder host and the media server host, the default path is correct.
11. Click **Next**.



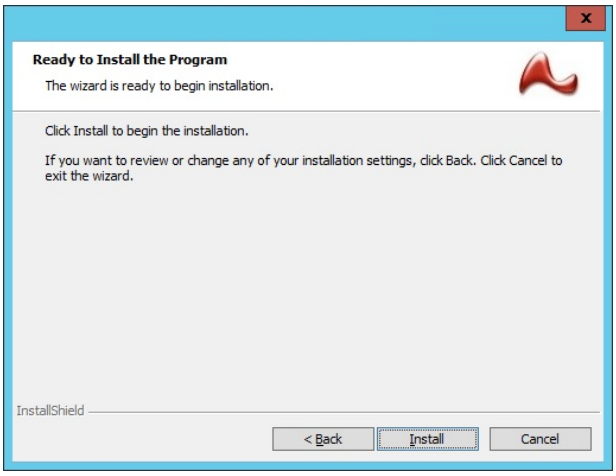
12. On the transcoder host, set the service identity to run as either **Local System** or as a **Specific User**.
    - Offers the benefit of already having proper access and no password management requirements.
    - Running as a **Specific User** offers the path of least privilege. However, it requires configuring NTFS permissions to read, write, and delete files on the **Source** directory.



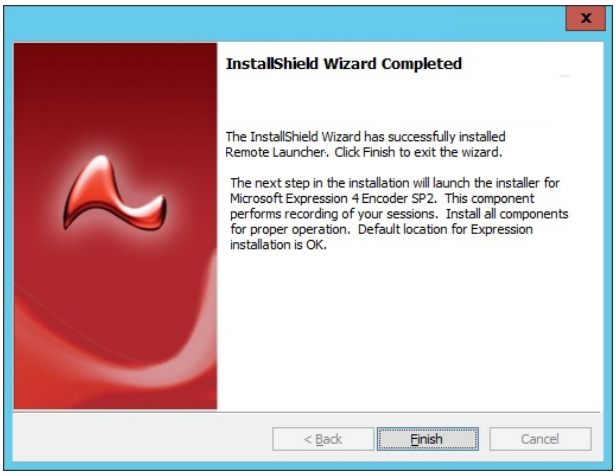
> ***Note:*** *On the transcoder host, running the* ***File Watcher service*** *as* ***Local System*** *is recommended.*

13. Click **Next**.

14. Click **Install**.



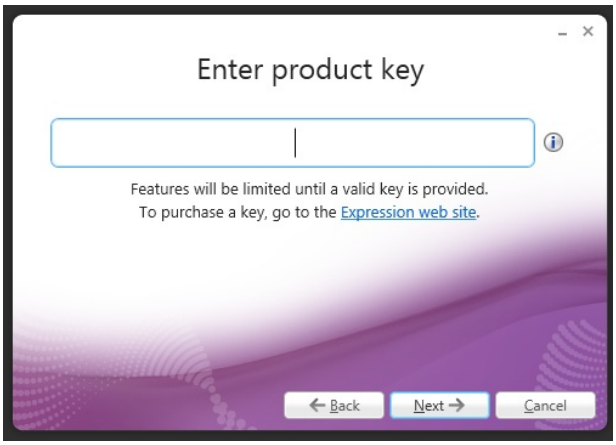
15. Click **Finish** to complete the first part of the installation. After the initial installation is complete, a separate installation for the Microsoft Expressions recorder is initiated.



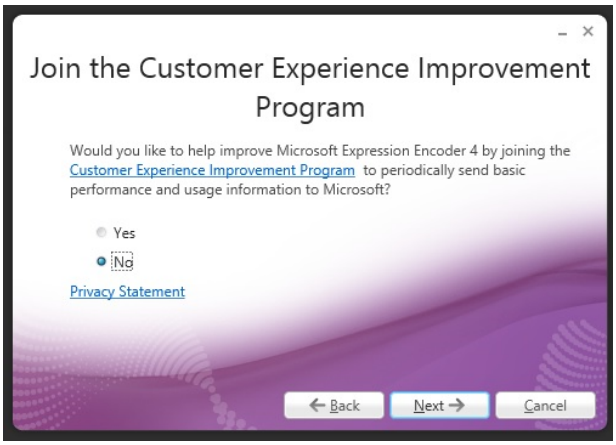
Install Microsoft Expressions Recorder

1. Accept the license agreement for the Microsoft Expressions recorder.

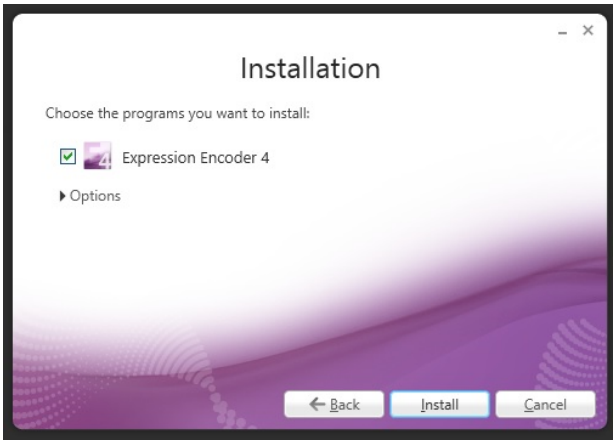
2. Click **Next** on the **Enter product key** page. No product key needs to be entered.



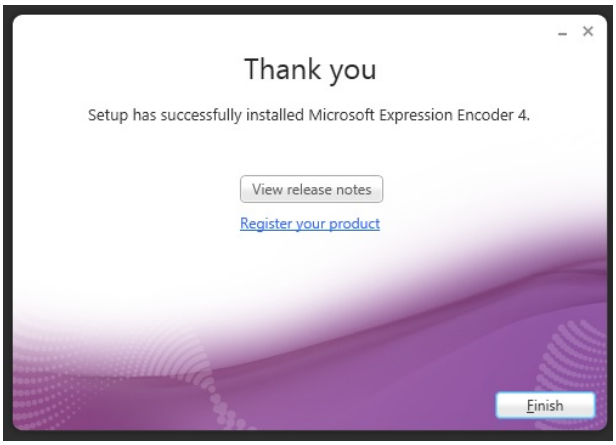
3. Choose if you would like to join the **Microsoft Customer Experience Improvement Program**. Click **Next**.



4. Select to install **Expression Encoder 4**. Click **Install**.



5. Click **Finish** to complete the installation.



6. Other tasks are performed that are not not visible in the installer, including:
    - A **[Domain] Local** security group is created called **WriteRecordingGroup**. If the installation is taking place on a domain controller, the group is created in the **Users** container. This group may be safely deleted from the jump server if also functioning as the transcoder host.
    - The **Domain Admins** group is added to this **WriteRecordingGroup**.
    - The installer creates and shares the following directory: **%inetpub%\wwwroot\SessionRecording** as **SessionRecording**. This directory is used to copy compiled session recordings from the jump server to the transcoder host. This scenario applies if using the FFMPeg video recorder rather than the Expressions recorder. This share directory will be required when configuring the jump server for app launching with session recording. If the transcoder and jump server are the same system, this share can be safely deleted.
    - The installer creates and shares the following directory: `%ProgramFiles(x86)%\Lieberman\Roulette\LaunchApp\Transcoders\Source` as **Source**. This directory is used by the jump server to copy raw session recording files to the transcoder host. This scenario would apply if using the Expressions 4 recording software. This share directory is required when configuring the jump server for app launching with session recording. If the transcoder and jump server are the same system, this share can be safely deleted.
    - Each of the shared directory's share permissions are set to allow full control of the **WriteRecordingGroup**. Minimum permission required is **Change**.

Install the Streaming Media Software on the Session Recording Media Server

IMPORTANT!

If you are not installing and using the session recording software, skip this step.

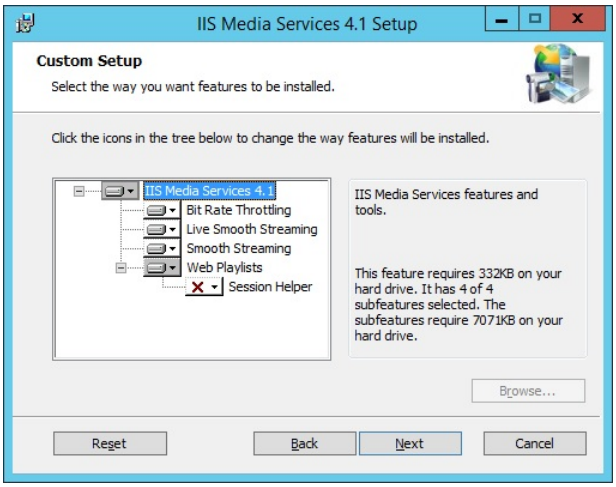
The streaming media services broadcast recorded sessions from the streaming host to the client's browser and video player.

Note: *The installation of IIS media services requires a basic installation of IIS to be available on the same host server.*

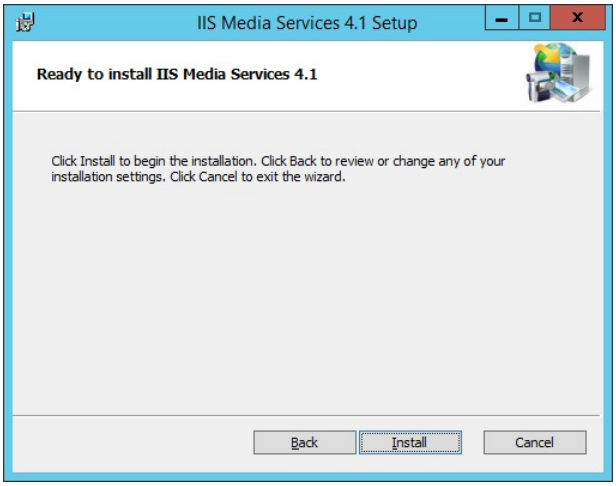
1. To begin installing the media software, open the **SupplementalInstallers** sub-folder from the installation directory, **%ProgramFiles (x86)\Lieberman\Roulette**.
2. Copy **IISMedia64.msi** to the machine functioning as the streaming video server, and launch the installer.
3. Click **Next** on the **Welcome** page.

4. Read and accept the terms of the license agreement. Click **Next**.

5. Leave the default options selected. Click **Next**.



6. Click **Install**.



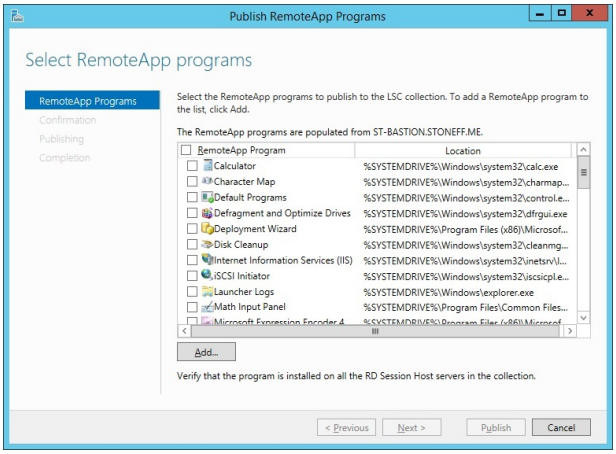
7. Click **Finish**.

Configure Remote Desktop Services (RDS) for Application Launching

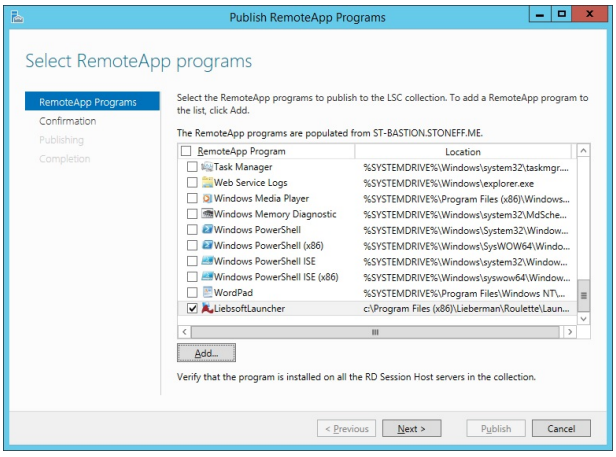
When a user uses the **Launch App** link in the web application, the launcher is called and obtains the necessary credential information for the application to launch. The application is launched from the jump server. In turn, VDI displays the remote application on the user's workstation like a local application. Before application launching can occur, RDS must be configured.

Configure Remote App

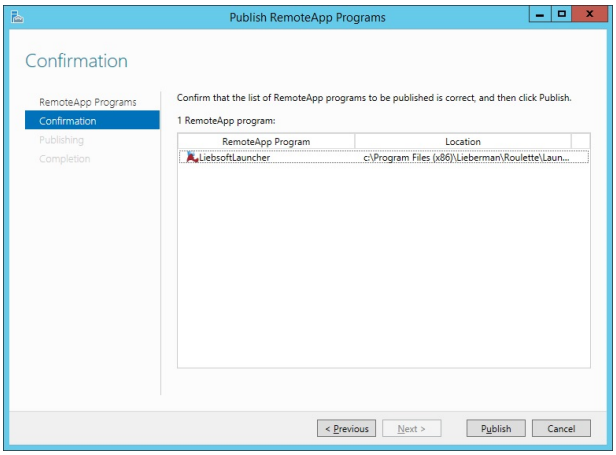
1. Open **Server Manager**. Select **Remote Desktop Services > Collections**.
2. Select the collection needed to configure application launcher.
3. In the **RemoteApp Programs** area, select **Tasks select > Publish RemoteApp Programs**.
4. Click **Add** on the **Publish RemoteApp programs** dialog.



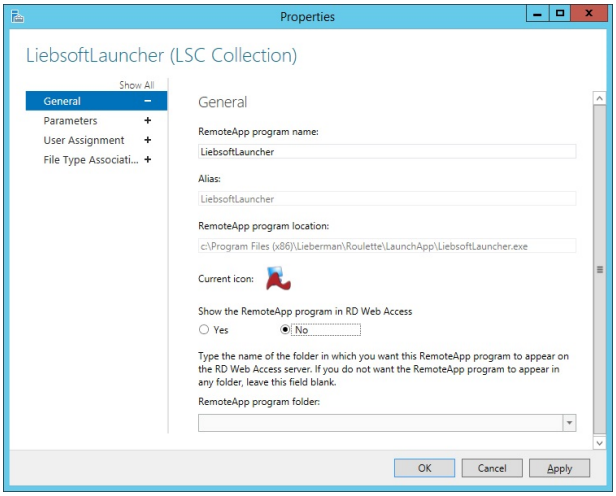
5. Select **LiebsoftLauncher.exe** from the application launcher installation location on the jump server. The default directory for this file is **C:\Program Files (x86)\Lieberman\Roulette\LaunchApp**.
6. Click **Next**.



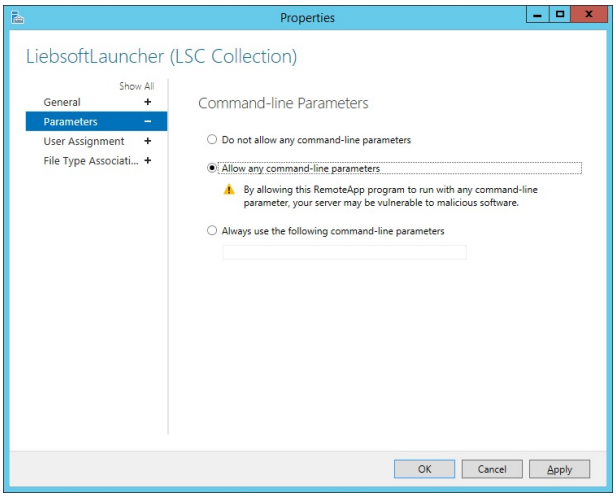
7. On the **Confirmation** page, click **Publish**.



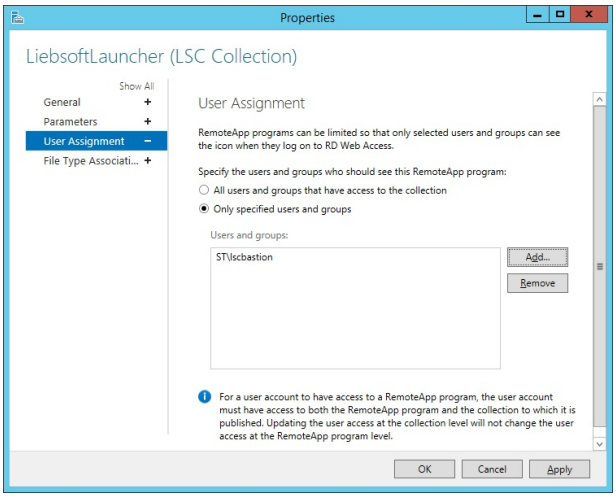
8. Once the **LiebsoftLauncher** application is published, right-click on it in the **RemoteApp Programs** list. Select **Edit Properties**.
9. On the **General** tab, set the **Show the RemoteApp program in RD Web Access** dialog to **No**.



10. On the **Parameters** tab, select **Allow any command-line parameters**.



11. On the **User Assignment** tab, we highly recommend that you change the **User Assignment** option to be a specific user or group of users. You will be connected to the server as a pre-designated account, which can be managed by Privileged Identity. This is the only account that requires access to run the program. The account assigned requires all permissions and rights to launch desired programs.
12. Click **OK**.



Configure IIS to Host Recorded Sessions

IMPORTANT!

If you are not installing and using the session recording software, skip this step.

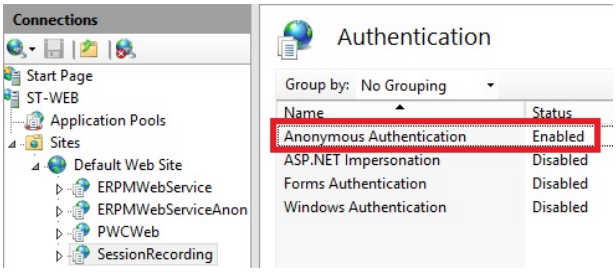
When an application is launched using a jump server and the application is configured to record sessions, the recorded sessions are placed into a pre-configured directory on the system. When using the Microsoft Expressions session recorder, the files are copied locally to the file system, and the **File Watcher** service moves the raw files to a share called **Source**. This machine is configured as the video transcoder in a XESC file. Once the raw XESC files are copied to the transcoder, the **File Watcher** service on the system transcodes the videos to WMV format and moves the compiled files into the **SessionRecording** share on the same system. This directory is hosted in IIS and is made available via the web application.

To configure IIS on the machine hosting the compiled videos, minimal configuration is required. The application launcher installer configures most of the required elements:

The default web site will have a new virtual directory added, called **SessionRecording**. This directory will point to **%inetpub%\wwwroot\SessionRecording**.

The only change that **may** need to be made is to set the authentication scheme to anonymous:

1. Open IIS and expand the **Default Web Site**.
2. Open the **Authentication** area.
3. Right-click on the **Authentication Types**.
4. Enable **Anonymous Authentication** and disable all others.



Configure the Application Launcher and Session Recorder

After installation, there are five configuration steps to complete before using the application launcher and the session recorder.

Configure the Jump Server Logon Account

The Application Launcher uses a standard logon account to log into the target jump server and launch the **LiebsoftLauncher** application. The **LiebsoftLauncher** application launches the target application and connects to a web service, **WebLauncherBackendService.svc**, to obtain the necessary program settings and credentials.

Logon Account Requirements

The logon account must have the following:

- A domain account is recommended, but the logon account can be a local account.
- The account must be able to remotely log into the target jump server. If the account is not an administrator, it must be added to the **Remote Desktop Users** group on the jump server.
- Because the user account launches the LiebsoftLauncher application upon login, make sure the account has the permissions required for launch. Set the permissions in the **RemoteApp** settings, which are found in **Server Manager > Roles > Remote Desktop Services**. The permissions can be assigned directly to the user or assigned to a group that the user belongs to.
- The account needs all of the same rights necessary to launch the final target application. It does not necessarily need local or domain admin privileges.

Secure the Logon Account

- The account for application launching should have its password rotated frequently by Privileged Identity. Daily or weekly is recommended; however, setting the rotation schedule to hourly is not recommended and could possibly invalidate the logon account's session.
- There are no requirements for password propagation, and it is recommended you turn off password propagation for the password change job.
- We recommend keeping the password length 80 characters or less because some versions of Windows will not allow longer passwords to be used with RDP.

IMPORTANT!

When launching an application, this account will be able to do anything the target application allows.

Recommended Policy Settings for the Logon Account

If this account is located in Active Directory, we recommend placing the account into an organizational unit (OU) by itself or with other similarly locked down accounts. On this OU, create a policy and modify the **User Settings** portion of the policy to lock down this logon account. There is no need to place the jump server in this OU because the policies locking down the user experience are user-based and not system-based.

The following table provides a list of recommended settings for lockdown. All policies should be tested to ensure they do not interfere with the required operation of a target application:

Policy	Setting
Enforcement	
Apply Software Restriction Policies to the following	All software files except libraries (such as DLLs)
Apply Software Restriction Policies to the following users	All users
When applying Software Restriction Policies	Ignore certificate rules
Trusted Publishers	
Trusted publisher management	Allow all administrators and users to manage user's own trusted publishers
Certificate verification	None
Software Restriction Policies > Security Levels	
Default Security Level	Disallowed
Software Restriction Policies > Additional Rules > Path Rules	
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%	Security Level = Unrestricted
%HKEY_LOCAL_ MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir%	Security Level = Unrestricted
C:\Program Files (x86)\Lieberman\Roulette\RemoteAppLauncher\LiebsoftLauncher.exe	Security Level = Unrestricted
User Configuration | Policies | Administrative Templates	
Control Panel	
Prohibit access to Control Panel and PC settings	Enabled
Control Panel > Display	
Disable the Display Control Panel	Enabled
Control Panel > Printers	
Browse a common web site to find printers	Disabled
Browse the network to find printers	Disabled
Prevent addition of printers	Enabled
Prevent deletion of printers	Enabled
Control Panel > Programs	
Hide "Get Programs" page	Enabled
Hide "Installed Updates" page	Enabled
Hide "Programs and Features" page	Enabled
Hide "Set Program Access and Computer Defaults" page	Enabled
Hide "Windows Features"	Enabled
Hide the Programs Control Panel	Enabled
Control Panel > Regional and Language Options	
Hide Regional and Language Options	Enabled
Hide the geographic location option	Enabled

Policy	Setting
Hide the select language group options	Enabled
Hide user locale selection and customization options	Enabled
Desktop	
Don't save settings at exit	Enabled
Hide and disable all items on the desktop	Enabled
Hide Internet Explorer icon on desktop	Enabled
Hide Network Locations icon on desktop	Enabled
Prevent adding, dragging, dropping and closing the Taskbar's toolbars	Enabled
Prohibit adjusting desktop toolbars	Enabled
Prohibit User from manually redirecting Profile Folders	Enabled
Remove Computer icon on the desktop	Enabled
Remove Properties from the Computer icon context menu	Enabled
Remove Properties from the Recycle Bin context menu	Enabled
Remove Recycle Bin icon from desktop	Enabled
Turn off Aero Shake window minimizing mouse gesture	Enabled
Network > Network Connections	
Ability to change properties of an all user remote access connection	Disabled
Prohibit access to properties of a LAN connection	Enabled
Prohibit access to the Remote Access Preferences item on the Advanced menu	Enabled
Prohibit changing properties of a private remote access connection	Enabled
Prohibit connecting and disconnecting a remote access connection	Enabled
Prohibit renaming private remote access connections	Enabled
Network > Offline Files	
Remove "Make Available Offline" command	Enabled
Remove "Work offline" command	Enabled
Network > Windows Connect Now	
Prohibit access to the Windows Connect Now wizards	Enabled
Start Menu and Taskbar	
Add Search Internet link to Start Menu	Disabled
Add the Run command to the Start Menu	Disabled
Clear history of recently opened documents on exit	Enabled
Clear history of tile notifications on exit	Enabled
Clear the recent programs list for new users	Enabled
Do not allow pinning items in Jump Lists	Enabled
Do not allow pinning programs to the Taskbar	Enabled
Do not display any custom toolbars in the taskbar	Enabled

Policy	Setting
Do not display or track items in Jump Lists from remote locations	Enabled
Do not keep history of recently opened documents	Enabled
Do not search communications	Enabled
Do not search for files	Enabled
Do not search Internet	Enabled
Do not search programs and Control Panel items	Enabled
Do not use the search-based method when resolving shell shortcuts	Enabled
Do not use the tracking-based method when resolving shell shortcuts	Enabled
Hide the notification area	Enabled
Lock all taskbar settings	Enabled
Lock the Taskbar	Enabled
Prevent changes to Taskbar and Start Menu Settings	Enabled
Prevent users from adding or removing toolbars	Enabled
Prevent users from moving taskbar to another screen dock location	Enabled
Prevent users from rearranging toolbars	Enabled
Prevent users from uninstalling applications from Start	Enabled
Remove access to the context menus for the taskbar	Enabled
Remove All Programs list from the Start menu	Enabled
Remove and prevent access to the Shut Down, Restart, Sleep, and Hibernate commands	Enabled
Remove Clock from the system notification area	Enabled
Remove common program groups from Start Menu	Enabled
Remove Default Programs link from the Start menu.	Enabled
Remove Documents icon from Start Menu	Enabled
Remove Downloads link from Start Menu	Enabled
Remove drag-and-drop and context menus on the Start Menu	Enabled
Remove Favorites menu from Start Menu	Enabled
Remove frequent programs list from the Start Menu	Enabled
Remove Games link from Start Menu	Enabled
Remove Help menu from Start Menu	Enabled
Remove Homegroup link from Start Menu	Enabled
Remove links and access to Windows Update	Enabled
Remove Logoff on the Start Menu	Disabled
Remove Music icon from Start Menu	Enabled
Remove Network Connections from Start Menu	Enabled
Remove Network icon from Start Menu	Enabled

Policy	Setting
Remove Pictures icon from Start Menu	Enabled
Remove pinned programs from the Taskbar	Enabled
Remove pinned programs list from the Start Menu	Enabled
Remove programs on Settings menu	Enabled
Remove Recent Items menu from Start Menu	Enabled
Remove Recorded TV link from Start Menu	Enabled
Remove Run menu from Start Menu	Enabled
Remove See More Results / Search Everywhere link	Enabled
Remove the Action Center icon	Enabled
Remove the battery meter	Enabled
Remove the networking icon	Enabled
Remove the volume control icon	Enabled
Remove user folder link from Start Menu	Enabled
Remove user's folders from the Start Menu	Enabled
Remove Videos link from Start Menu	Enabled
Show "Run as different user" command on Start	Disabled
Turn off all balloon notifications	Enabled
Turn off automatic promotion of notification icons to the taskbar	Enabled
Turn off feature advertisement balloon notifications	Enabled
Turn off notification area cleanup	Enabled
Turn off user tracking	Enabled
Start Menu and Taskbar > Notifications	
Turn off notifications network usage	Enabled
System > Ctrl+Alt+Del Options	
Remove Change Password	Enabled
Remove Task Manager	Enabled
System > Internet Communication Management > Internet Communication settings	
Turn off access to the Store	Enabled
Turn off downloading of print drivers over HTTP	Enabled
Turn off handwriting recognition error reporting	Enabled
Turn off Help Experience Improvement Program	Enabled
Turn off Help Ratings	Enabled
Turn off Internet download for Web publishing and online ordering wizards	Enabled
Turn off Internet File Association service	Enabled
Turn off printing over HTTP	Enabled
Turn off the "Order Prints" picture task	Enabled

Policy	Setting
Turn off the "Publish to Web" task for files and folders	Enabled
Turn off the Windows Messenger Customer Experience Improvement Program	Enabled
Turn off Windows Online	Enabled
System > Removable Storage Access	
All Removable Storage classes: Deny all access	Enabled
CD and DVD: Deny read access	Enabled
CD and DVD: Deny write access	Enabled
Floppy Drives: Deny read access	Enabled
Floppy Drives: Deny write access	Enabled
Removable Disks: Deny read access	Enabled
Removable Disks: Deny write access	Enabled
Tape Drives: Deny read access	Enabled
Tape Drives: Deny write access	Enabled
WPD Devices: Deny read access	Enabled
WPD Devices: Deny write access	Enabled
System > Windows HotStart	
Turn off Windows HotStart	Enabled
Windows Components > Add features to Windows 8	
Prevent the wizard from running.	Enabled
Windows Components > App runtime	
Block launching desktop apps associated with a file.	Enabled
Block launching desktop apps associated with a protocol	Enabled
Windows Components > Application Compatibility	
Turn off Program Compatibility Assistant	Enabled
Windows Components > Attachment Manager	
Hide mechanisms to remove zone information	Enabled
Windows Components > AutoPlay Policies	
Disallow Autoplay for non-volume devices	Enabled
Prevent AutoPlay from remembering user choices.	Enabled
Set the default behavior for AutoRun	Enabled
Default AutoRun Behavior (Do not execute any autorun commands)	
Turn off Autoplay	Enabled
Turn off Autoplay on	All drives
Windows Components > Credential User Interface	
Do not display the password reveal button	Enabled

Policy	Setting
Windows Components > Desktop Gadgets	
Restrict unpacking and installation of gadgets that are not digitally signed.	Enabled
Turn off desktop gadgets	Enabled
Turn Off user-installed desktop gadgets	Enabled
Windows Components > Digital Locker	
Do not allow Digital Locker to run	Enabled
Windows Components > Edge UI	
Turn off switching between recent apps	Enabled
Turn off tracking of app usage	Enabled
Windows Components > File Explorer	
Display confirmation dialog when deleting files	Enabled
Display the menu bar in File Explorer	Enabled
Do not allow Folder Options to be opened from the Options button on the View tab of the ribbon	Enabled
Do not display the Welcome Center at user logon	Enabled
Do not request alternate credentials	Enabled
Hide these specified drives in My Computer	Enabled
Restrict all drives	
Hide the Manage item on the File Explorer context menu	Enabled
No Entire Network in Network Locations	Enabled
Prevent access to drives from My Computer	Enabled
Restrict all drives	
Prevent users from adding files to the root of their Users Files folder.	Enabled
Remove "Map Network Drive" and "Disconnect Network Drive"	Enabled
Remove CD Burning features	Enabled
Remove File Explorer's default context menu	Enabled
Remove File menu from File Explorer	Enabled
Remove Hardware tab	Enabled
Remove Security tab	Enabled
Remove the Search the Internet "Search again" link	Enabled
Turn off display of recent search entries in the File Explorer search box	Enabled
Turn off Windows+X hotkeys	Enabled
Windows Components > File Explorer > Common Open File Dialog	
Hide the common dialog back button	Enabled
Hide the common dialog places bar	Enabled
Hide the dropdown list of recent files	Enabled

Policy	Setting
Windows Components > File Explorer > Explorer Frame Pane	
Turn off Preview Pane	Enabled
Turn on or off details pane	Enabled
Configure details pane	Always hide
Windows Components > File Explorer > Previous Versions	
Prevent restoring previous versions from backups	Enabled
Windows Components > IME	
Turn off history-based predictive input	Enabled
Turn off Internet search integration	Enabled
Windows Components > Internet Explorer	
Automatically activate newly installed add-ons	Disabled
Configure Media Explorer Bar	Enabled
Disable the Media Explorer Bar and auto-play feature	Enabled
Auto-Play Media files in the Media bar when Enabled	Disabled
Disable AutoComplete for forms	Enabled
Disable changing accessibility settings	Enabled
Disable changing Advanced page settings	Enabled
Disable changing Automatic Configuration settings	Enabled
Disable changing Calendar and Contact settings	Enabled
Disable changing certificate settings	Enabled
Disable changing connection settings	Enabled
Disable changing home page settings	Enabled
Home Page	Define a home page if necessary
Disable changing language settings	Enabled
Disable changing Messaging settings	Enabled
Disable changing ratings settings	Enabled
Disable changing Temporary Internet files settings	Enabled
Disable Import/Export Settings wizard	Enabled
Disable Internet Connection wizard	Enabled
Do not allow users to enable or disable add-ons	Enabled
Identity Manager: Prevent user from using Identities	Enabled
Notify users if Internet Explorer is not the default web browser	Disabled
Pop-up allow list	Enabled
Enter the list of sites here.	Define allowed sites list if applicable such as *.microsoft.com
Prevent "Fix settings" functionality	Enabled
Prevent access to Internet Explorer Help	Enabled

Policy	Setting
Prevent bypassing SmartScreen Filter warnings	Enabled
Prevent bypassing SmartScreen Filter warnings about files that are not commonly downloaded from the Internet	Enabled
Prevent changing pop-up filter level	Enabled
Prevent changing proxy settings	Enabled
Prevent changing the default search provider	Enabled
Prevent configuration of how windows open	Enabled
Select where to open links	Open in existing Internet Explorer window
Prevent Internet Explorer Search box from appearing	Enabled
Prevent managing pop-up exception list	Enabled
Prevent managing SmartScreen Filter	Enabled
Select SmartScreen Filter mode	On
Prevent participation in the Customer Experience Improvement Program	Enabled
Prevent per-user installation of ActiveX controls	Enabled
Prevent running First Run wizard	Enabled
Select your choice	Go directly to home page
Search: Disable Find Files via F3 within the browser	Enabled
Search: Disable Search Customization	Enabled
Specify default behavior for a new tab	Enabled
New tab behavior	Home page
Turn off ability to pin sites in Internet Explorer on the desktop	Enabled
Turn off add-on performance notifications	Enabled
Turn off browser geolocation	Enabled
Turn off configuration of pop-up windows in tabbed browsing	Enabled
Select tabbed browsing pop-up behavior	Force pop-ups to open in a new tab
Turn off Crash Detection	Enabled
Turn off Favorites bar	Enabled
Turn off Managing SmartScreen Filter for Internet Explorer 8	Enabled
Select SmartScreen Filter mode for Internet Explorer 8	On
Turn off pop-up management	Enabled
Turn off Quick Tabs functionality	Enabled
Turn off Reopen Last Browsing Session	Enabled
Turn off suggestions for all user-installed providers	Enabled
Turn off tabbed browsing	Enabled
Turn off the auto-complete feature for web addresses	Enabled
Turn off the quick pick menu	Enabled

Policy	Setting
Turn on Suggested Sites	Disabled
Turn on the auto-complete feature for user names and passwords on forms	Disabled
Windows Components > Internet Explorer > Accelerators	
Turn off Accelerators	Enabled
Windows Components > Internet Explorer > Browser menus	
Disable Open in New Window menu option	Enabled
Disable Save this program to disk option	Enabled
File menu: Disable closing the browser and Explorer windows	Enabled
File menu: Disable New menu option	Enabled
File menu: Disable Open menu option	Enabled
File menu: Disable Save As Web Page Complete	Enabled
File menu: Disable Save As... menu option	Enabled
Help menu: Remove 'Send Feedback' menu option	Enabled
Help menu: Remove 'Tour' menu option	Enabled
Hide Favorites menu	Enabled
Tools menu: Disable Internet Options... menu option	Enabled
Turn off Print Menu	Enabled
Turn off Shortcut Menu	Enabled
View menu: Disable Full Screen menu option	Enabled
View menu: Disable Source menu option	Enabled
Windows Components > Internet Explorer > Delete Browsing History	
Disable "Configuring History"	Enabled
Days to keep pages in History	1
Windows Components > Internet Explorer > Internet Control Panel	
Disable the Advanced page	Enabled
Disable the Connections page	Enabled
Disable the Content page	Enabled
Disable the General page	Enabled
Disable the Privacy page	Enabled
Disable the Programs page	Enabled
Disable the Security page	Enabled
Windows Components > Internet Explorer > Internet Control Panel > Advanced Page	
Allow active content from CDs to run on user machines	Disabled
Allow software to run or install even if the signature is invalid	Disabled
Do not allow resetting Internet Explorer settings	Enabled
Empty Temporary Internet Files folder when browser is closed	Enabled

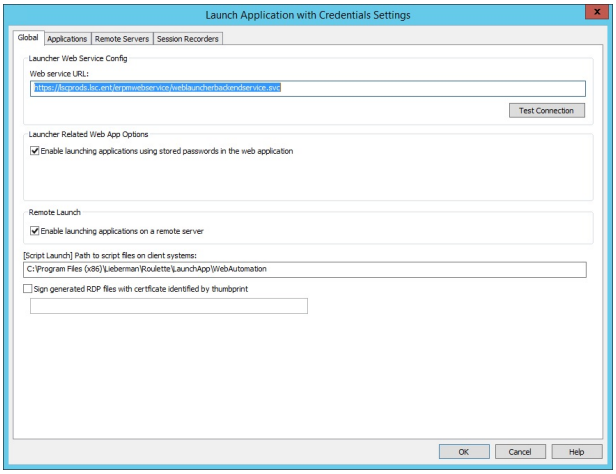
Policy	Setting
Windows Components > Internet Explorer > Internet Control Panel > General Page	
Start Internet Explorer with tabs from last browsing session	Disabled
Windows Components > Internet Explorer > Internet Control Panel > General Page > Browsing History	
Allow web sites to store application caches on client computers	Disabled
Windows Components > Internet Explorer > Internet Settings > Advanced Settings > Browsing	
Turn off details in messages about Internet connection problems	Enabled
Turn on script debugging	Disabled
Windows Components > Internet Explorer > Internet Settings > Advanced Settings > Multimedia	
Allow Internet Explorer to play media files that use alternative codecs	Disabled
Windows Components > Internet Explorer > Internet Settings > Advanced Settings > Searching	
Prevent configuration of search on Address bar	Enabled
When searching from the address bar	Do not search from the address bar
Prevent configuration of top-result search on Address bar	Enabled
When searching from the Address bar	Disable top result search
Windows Components > Internet Explorer > Internet Settings > Advanced settings > Signup Settings	
Turn on automatic signup	Disabled
Windows Components > Internet Explorer > Internet Settings > AutoComplete	
Turn off URL Suggestions	Enabled
Turn off Windows Search AutoComplete	Enabled
Turn on inline AutoComplete	Disabled
Windows Components > Internet Explorer > Security Features > Restrict File Download	
All Processes	Enabled
Internet Explorer Processes	Enabled
Windows Components > Internet Explorer > Toolbars	
Configure Toolbar Buttons	Enabled
Show Back button	Enabled
Show Forward button	Enabled
Show Stop button	Enabled
Show Refresh button	Enabled
Show Home button	Enabled
Show Search button	Disabled
Show Favorites button	Disabled
Show History button	Disabled
Show Folders button	Disabled
Show Fullscreen button	Disabled
Show Tools button	Disabled
Show Mail button	Disabled

Policy	Setting
Show Font size button	Disabled
Show Print button	Disabled
Show Edit button	Disabled
Show Discussions button	Disabled
Show Cut button	Disabled
Show Copy button	Disabled
Show Paste button	Disabled
Show Encoding button	Disabled
Disable customizing browser toolbar buttons	Enabled
Disable customizing browser toolbars	Enabled
Display tabs on a separate row	Enabled
Hide the Command bar	Enabled
Hide the status bar	Enabled
Lock all toolbars	Enabled
Lock location of Stop and Refresh buttons	Enabled
Turn off Developer Tools	Enabled
Turn off toolbar upgrade tool	Enabled
Windows Components > Location and Sensors	
Turn off location	Enabled
Windows Components > Microsoft Management Console	
Restrict the user from entering author mode	Enabled
Windows Components > Network Sharing	
Prevent users from sharing files within their profile.	Enabled
Windows Components > Presentation Settings	
Turn off Windows presentation settings	Enabled
Windows Components > Sound Recorder	
Do not allow Sound Recorder to run	Enabled
Windows Components > Tablet PC > Accessories	
Do not allow printing to Journal Note Writer	Enabled
Do not allow Snipping Tool to run	Enabled
Do not allow Windows Journal to run	Enabled
Windows Components > Tablet PC > Hardware Buttons	
Prevent Back-ESC mapping	Enabled
Prevent launch an application	Enabled
Prevent press and hold	Enabled
Turn off hardware buttons	Enabled

Policy	Setting
Windows Components > Windows Error Reporting	
Disable Windows Error Reporting	Enabled
Windows Components > Windows Installer	
Prevent removable media source for any installation	Enabled
Prohibit rollback	Enabled
Windows Components > Windows Logon Options	
Set action to take when logon hours expire	Enabled
Set action to take when logon hours expire	Logoff
Windows Components > Windows Mail	
Turn off the communities features	Enabled
Turn off Windows Mail application	Enabled
Windows Components > Windows Media Center	
Do not allow Windows Media Center to run	Enabled
Windows Components > Windows Media Player	
Prevent CD and DVD Media Information Retrieval	Enabled
Prevent Music File Media Information Retrieval	Enabled
Windows Components > Windows Media Player > Networking	
Hide Network Tab	Enabled
Windows Components > Windows Media Player > Playback	
Prevent Codec Download	Enabled
Windows Components > Windows Messenger	
Do not allow Windows Messenger to be run	Enabled
Do not automatically start Windows Messenger initially	Enabled
Windows Components > Windows Mobility Center	
Turn off Windows Mobility Center	Enabled
Windows Components > Windows Update	
Do not adjust default option to 'Install Updates and Shut Down' in Shut Down Windows dialog box	Enabled
Do not display 'Install Updates and Shut Down' option in Shut Down Windows dialog box	Enabled

Configure the Web Launcher Settings

1. To configure the web launcher settings for the web application, open the management console.
2. Go to **Settings > Manage Web Application > Application Launch** in the management console.
3. The **Launch Application with Credentials Settings** dialog opens. The **Global** tab identifies the URL for the web service and other related settings used when launching applications.



4. Enter the web service URL.
   - **Web service URL:** The URL of the application launcher web service. When the web service is installed, a web service is created at **[site]/erpmwebservice**. The web service is called **WebLauncherBackendService.svc**. Enter the full URL in the **Web service URL** field, including the protocol and port if applicable. The typical URL is:

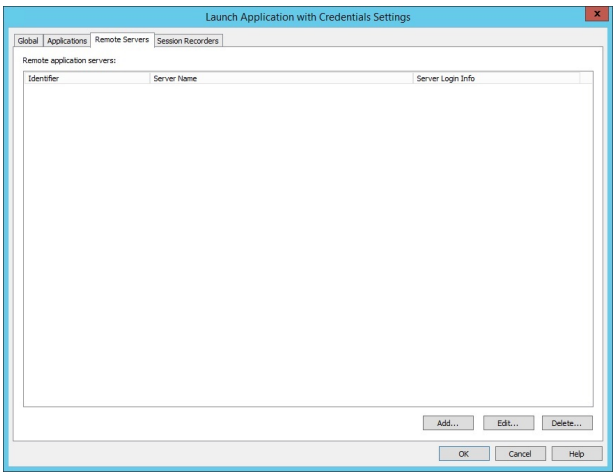
     https://erpmwebservername.example.com/erpmwebservice/weblauncherbackendservice.svc.
   - Click **Test Connection** to verify the web service URL is correct and the web service is properly responding to requests.
5. Check the **Enable launching applications using stored passwords in the web application** box. This option enables remote launching. If this option is not selected, the **Launch Application** option is unavailable in the website.
6. Check the **Enable launching applications on a remote server** box. This option enables configured applications to launch via the jump server rather than launching locally on the client. When the option is enabled and an application is configured to use the jump server, the applications launch from the jump server and use RemoteApp to display the program's user interface to the user's desktop.
7. Enter the path where the script automation files will be copied to in the **[Script Launch] Path to script files on client systems** field . This path is used when locally launching web-based applications.. If local launching will not be used, you do not need to configure a path. The default location where these scripts are found is **C:\Program Files (x86)\Lieberman\Roulette\LaunchApp\WebAutomation**.
8. When RDP files are generated, they are signed with the identified certificate. This helps avoid unknown/untrusted RDP connection warnings and errors. For the **Sign generated RDP files with certificate identified by thumbprint** option to function, the following must be true:
   - The certificate must be on the client workstation to generate RDP files and connect to the jump server.
   - If RDP connections are configured to go through the jump server, the certificate also must be on the jump server.
   - The certificate must be accessible to the user running the process of creating and launching the RDP file.
   - The security policy of the machine must be configured to require signed RDP files for this setting to have any effect.

Configure the Jump Server Settings

1. From the management console, go to **Settings > Manage Web Application > Application Launch** in the management console.
2. Select **Remote Servers**.

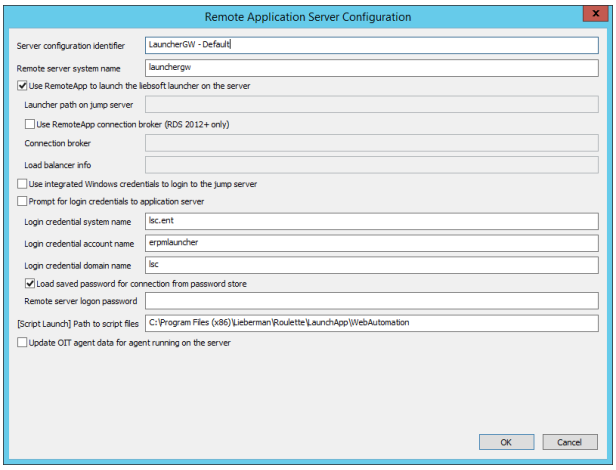
Configuring Remote Servers

The **Remote Servers** tab identifies the available jump servers and other related settings used for launching applications. The option **Enable launching applications on a remote server** must also be selected on the **Global** tab to make use of these servers. The first time this dialog is opened no remote servers will be available for application launching.



To add a new server, click **Add**.

The following fields are mandatory:



- **Server configuration identifier:** The friendly name of the server.
- **Remote server system name:** The actual name of the jump server. This should be the name (FQDN, simple name, or IP) that can be reached from the client systems initiating the sessions.
- **Use RemoteApp to launch the liebsoft launcher on the server:** This option must be selected to remotely launch applications from the jump server using RemoteApp.
    - **Launcher path on jump server:** The path to the launcher on the jump server. If the option **Use RemoteApp to launch the liebsoft launcher on the server** is enabled, this option is unavailable.
    - **Use RemoteApp connection broker (RDS 2012+ only)**
        - **Connection broker:** The fully qualified domain name (FQDN) of the connection broker, such **as 2k12r2-3.demo.msft**.
        - **Load balancer info:** The **loadbalanceinfo** value from the .rdp file, such as **tsv://MS Terminal Services Plugin.1.lsc.example**.

IMPORTANT!

*Make sure your RDS collection name does not exceed 16 characters. Microsoft truncates names exceeding 16 characters when storing the name in the registry. If the truncated name does not match the configured **load balancer** info value, the following error message is returned "Your computer can't connect to the remote computer because the connection broker couldn't validate the settings in your RDP file."*

- **Use integrated Windows credentials to login to the jump server:** This feature connects to the jump server using user credentials rather than a specific jump server login. This occurs when the following requirements are met:
  - The jump server is properly configured for web single-server sign-on
  - The web application is also configured for use with integrated authentication
  - The user logs in using integrated authentication
  - The login user has permissions to launch the application and RDP to the server
- **Prompt for login credentials to application server:** This prevents credentials from being automatically provided when connecting to the jump server. The user performing the application launch must provide credentials for the jump server.
  - **Login credential system name:** Enter the name of the system as it appears in BeyondTrust Privileged Identity. If the application launcher is using stored (managed) credentials to log into the jump server, this field must be completed. It is recommended to use a domain credential for this purpose.
  - **Login credential account name:** Enter the name of the account used to log in to the jump server. It is recommended to use a domain credential for this purpose.
  - **Login credential domain name:** Enter the domain the account belongs to.
  - **Load saved password for connection from password store:** Select this option to pull managed passwords from the password store. To use a hard-coded password, enter the actual password in the remote server logon password field.
  - **[Script Launch] Path to script files on client systems:** Enter the path to the script automation files. This path is used when launching web-based applications. The default location for these scripts is **C:\Program Files (x86)\Lieberman\Roulette\LaunchApp\WebAutomation**.
- **Update OIT agent data for agent running on the server:** Select this option to change certain metadata attributes to reflect which user account is performing certain actions. This functionality works with ObserveIT only and affects auditing information stored within ObserveIT.

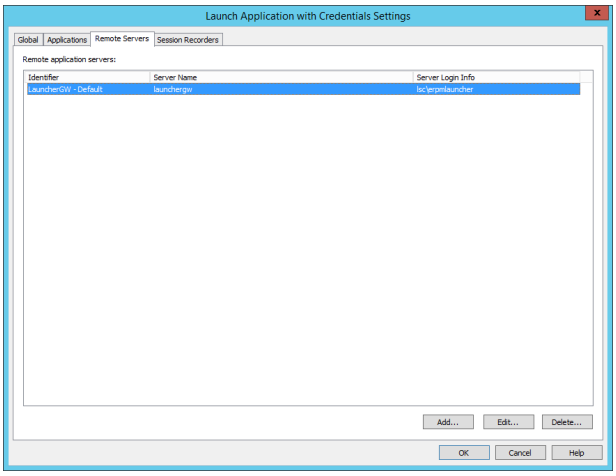
IMPORTANT!

*If using the built-in session recording from BeyondTrust instead of the ObserveIT session recorder, refrain from checking the **Update OIT agent data for agent running on the server** option. Checking this option prevents the built-in session recorder from operating.*

Once the entries are validated, click **OK**.

> ***Note:*** *If the option to* ***Load saved password for connection from password store*** *is selected and a stored password for the target account doesn't exist, a warning appears.*

All of these settings can be changed at any time without having to make any changes to IIS, performing IISReset, or other administrative actions.



Configure the Jump Server Host

This section lists two configuration updates to implement for the jump server host.

Configure the Jump Server for Multiple Application Launcher Sessions

The following configuration change is needed to allow multiple application launcher sessions to run concurrently.

1. Log into the jump server.
2. Open the **Run** dialog using the **Win+R** keyboard shortcut.
3. Type **gpedit.msc** and press **OK**. The **Local Group Policy Editor** window opens.
4. Choose **Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Connections : Restrict Remote Desktop Services users to a single Remote Desktop Services session**.
5. Right-click **Restrict Remote Desktop Services users to a single Remote Desktop Services session**.
6. Choose **Edit**, and a dialog opens to configure the policy.
7. Select **Disabled**.
8. Click **OK**.

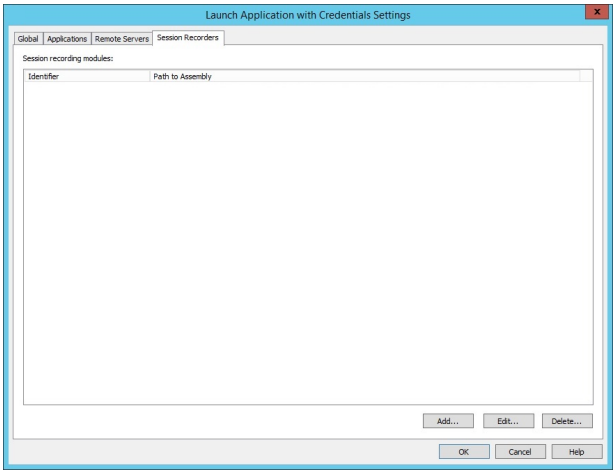
Prevent Transcoder Issues

The following configuration change is needed to prevent an issue resulting in your session recordings failing to be processed by the transcoder.

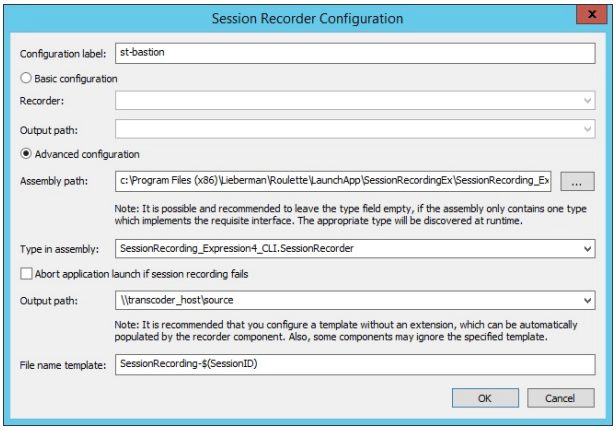
1. Open the **Run** dialog on the jump server using the **Win+R** keyboard shortcut.
2. Type **gpedit.msc** and press **OK**. The **Local Group Policy Editor** window opens.
3. Choose **Computer Configuration > Administrative Templates > System > User Profiles: Do not forcefully unload the user registry at logoff**.
4. Right-click **Do not forcefully unload the user registry at logoff**.
5. Choose **Edit**, and a dialog opens to configure the policy.
6. Select **Enabled**.
7. Click **OK**.

Configure Session Recording Settings

1. From the management console, go to **Settings > Manage Web Application > Application Launch**.
2. Select **Session Recorders**. The **Session Recorders** tab displays configured session recording servers. There is a one-to-one relationship with the servers configured on the **Remote Servers** tab.
3. To add a new server, click **Add...**. The following fields are mandatory:



   - **Configuration label:** Friendly name of the server to appear in the Application Launcher configuration.
   - **Basic configuration:** Check this option if the session recording host will perform both recording and transcoding duties. Recorder options include **Expressions 4**, **VLC**, and **Windows Problem Steps Recorder**. It is recommended to choose the Expressions 4 recorder option.
   - **Advanced configuration:** Check this option to put recordings in a custom location or if video transcoding will occur on a separate host. We do not recommended changing the **Assembly path** or **Type** in **Assembly values**.

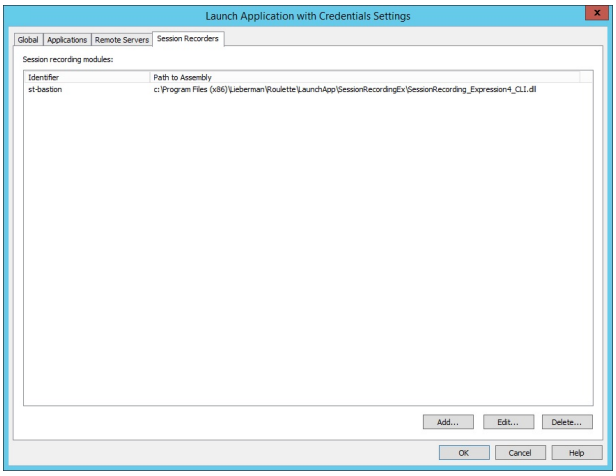


   - **Abort application launch if session recording fails:** Check this option if you prefer remote sessions to log off and not launch the remote app when session recording fails.
   - **Output path:** Enter the path for the system where raw session recording files will be stored. If using the jump server for both session recording and video transcoding, specify a local path. The default location is **c:\ProgramFiles (x86)\Lieberman\Roulette\LaunchApp\Transcoders\Source**. If the transcoder is on a separate host, specify the universal naming convention (UNC) path to the **Source** share on that server (**\\server\source**).

> ***Note:*** *Do not place a back slash after the last directory name.*

   - **File name template:** The default value is **SessionRecording-$(SessionID)**. **SessionRecording-** is the filename prefix, and **$(SessionID)** is the variable for the remote app launch session's session ID. You can change the names, but you should not remove the **$(SessionID)** value from the name. Also, an extension should not be listed for the file name.

Once the entries are validated, click **OK** to add the session recorder host object. Any of these settings can be changed at any time without having to make any changes to IIS or performing IISReset or other administrative actions.



Configure the Transcoder to Record Multiple Videos Simultaneously

By default, the session recording transcoder is set to record a maximum of one video at a time. To configure the transcoder to record multiple concurrent videos, complete the following steps.

1. Go to the system where the Application Launcher and Session Recorder components are installed.
2. Choose **Start > BeyondTrust > Settings**.
3. If necessary, expand the **File Watcher Transcoder Service Settings** section and locate **Setting: Maximum Concurrent Encoders**.
4. Enter the maximum number of simultaneous recordings the transcoder should allow. Click **Push**.
5. Close **Session Recording Configuration**.

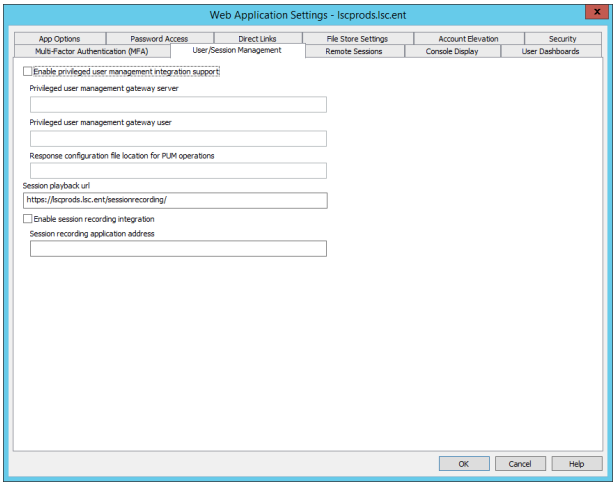
Configure the Web Application Settings for Session Playback

To playback recorded sessions, the web application must have the video playback URL where the final recorded sessions are stored.

Under the default root website, the media server configures IIS with a virtual directory called **SessionRecording**. This URL should be provided on the **User/Session Management** dialog. The **SessionRecording** URL may be presented with or without SSL but should use anonymous authentication.

Configure the Session Playback URL

1. Open the management console. Click **Manage Web App**.
2. Double-click an existing web application to edit. Or, change the default options by opening **Options > Configure default web application options**.
3. Click **User/Session Management**.
4. Locate the **Session playback URL** field and enter the URL for the media server. If using HTTPS, make sure to enter the valid name of the server matching the assigned name on the certificate to avoid certificate errors. A typical URL is similar to **https://server.example/sessionrecording/**. Be aware that the system is expecting a trailing forward slash at the end of the URL.
5. Click **OK**.
6. If updating an existing website with this new information, click **OK**. The new settings are pushed to the web instance and its COM application is restarted. If changing the default web application settings, right-click on the website instance and select **Replace instance options with default web application options**. After making this change, there is no need to restart any systems.



Once the URL is added and sessions have been recorded, users with access to the **Auditing** section of the web application are able to play back recorded sessions.

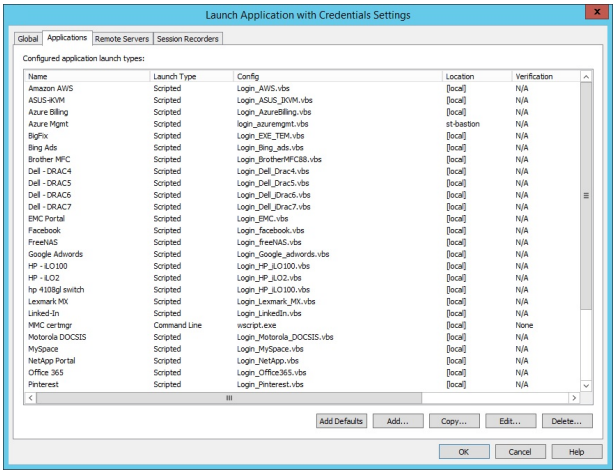
Configure Applications for Launching

This section describes how to configure applications for Application Launcher use.

Add Application Launching Scripts

Privileged Identity includes a number of application launching scripts. Most scripts require additional configuration before they can be used to launch applications.

1. In the management console, choose **Settings > Manage Web Application > Application Launch**.
2. Click **Applications**.
3. Click **Add Defaults**.
4. To add new applications, click the **Add** button. Duplicate or edit existing items by clicking **Copy** or **Edit**. After adding an application, you must configure the application.



Configuring Privileged Identity to Launch Applications

Configure Privileged Identity to Launch Specific Applications

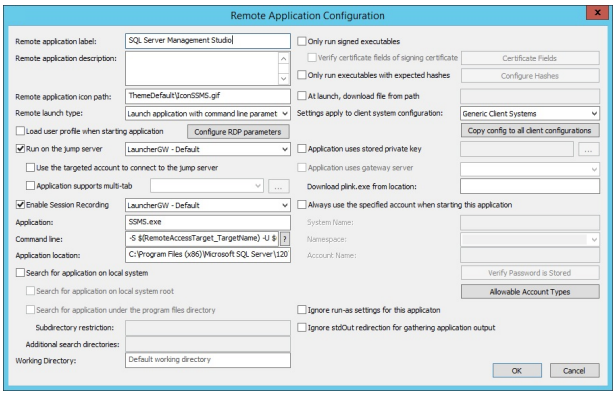
1. Open the management console.
2. Choose **Settings > Manage Web Application > Application Launch**.
3. Click **Applications**. The **Applications** tab displays applications that can be launched from the web application and other related settings.
4. Select an **Application Launch Type item**.
5. Click **Edit**.
6. Complete the form.

Edit the Remote Application Configuration

- **Remote application label:** *(Required)* Friendly name of the application as it will appear in the web application.
- **Remote application description:** *(Optional)* Enter a description for the application.
- **Remote application icon path:** *(Optional)* To set a custom icon for the application, identify the location of the physical web application installation files, **%inetpub%\wwwroot\PWCWeb**. All file paths defined for the icons are relative to this path. It is recommended to create a custom folder and add your icons to this folder to persist through website upgrades. Then, for the icon path, add the path using the following convention, **FolderName\IconName.gif**. All GIF files should be 32x32 pixels.
- **Remote launch type:***(Required)* Select from the available launch types:
    - **Launch application with command line parameters:** Select if this application can be launched with command line options, such as SQL Management Studio, PuTTY, VMware vCenter, etc.
    - **Open web application with form post:** Select if the website requires a basic form post and does not make use of JSON, YAML, or other technologies for passing username and password information. When selected, fill out the **Web Page** and **Name-Value pair** fields. The webpage is the name of the login page, including the protocol, such as **http://server.example/pwcweb/login.asp**, and the name-value pair should consist of the variables for the username and password.
    - **Launch terminal services client:** Select if launching the **Microsoft Terminal Services** client.
    - **Launch app through .NET assembly:** Select if an external .NET assembly will be used to connect and pass credentials. Enter the **Assembly Path** and **Type Name** values. The **Assembly Path** is the full physical file path to the .NET assembly, and the **Type Name** is the name of the .NET interface.
    - **Launch app through script automation:** Select if launching MMCs or websites not passing username and password information from a basic form post, thick clients not using command line parameters, etc. Enter the **Script Path** and **Automation URL**. **Script Path** is the script name, including the extension. For example, **login_azuremgmt.vbs**. This script must be found in the pre-defined script automation directory on the global options or Application Launch Server configuration dialogs for the app launcher. Automation URL is the target URL. For example, **http://manage.windowsazure.com** or for a device, **https://$(RemoteAccessTarget_TargetName)/login.html**.
- **Run on the jump server:** *(Optional)* Select if launching the target application from the jump server or from the user's workstation. If this option is not selected, the application attempts to launch from the user's local workstation. If selected, the application launches from the jump server. The application must be installed on the jump server. This is a per-application setting.
    - **Use the targeted account to connect to the jump server:** Select if a connection needs to be established with a domain account or a local jump server account. If a jump server is used and the account being targeted to launch the application is a domain account or a valid local account, this option will establish a connection with those credentials rather than the pre-configured jump server connection credentials. Do not use this option for non-Windows systems.

  - **Application supports multi-tab:** Select to enable a special set of configurations and launch scripts for applications with multi-branch or multi-tab capabilities.
  - **Load user profile when starting application (Configure RDP connection parameters):** Select if you wish to load the connecting user's user profile on the jump server, which enables additional items, such as color depth, mapped drives, clipboard capability, etc.

- **Enable session recording:** *(Optional)* If session recording is configured, this option is available. Select if launching this application on a jump server should initiate session recording, and record only this application being run. This is a per-application setting.
- **Application:** *(Required)* Enter the application name, which is the name of the executable without the path.
- **Command line:** *(Required)* Enter the command line parameters to launch the executable with. Parameters are specific to the program being launched and not Privileged Identity. Specific replacement variables are provided by Privileged Identity, which can be used in place of otherwise static values.
- **Application location:** *(Optional)* Define the application location. It can be a full physical path, or set up to search for and even download a ready-to-run executable from a predefined network path . A physical path MUST be defined when launching the application from a jump server. If a physical path is not defined in the application location field, the option to **Search for application on local system** should be enabled. Sub-options for application search include searching for the application on the system root or Program Files directories. In addition, subsequent include and exclude directories may be defined. Multiple values should be separated by a semicolon. There are no variable replacements, such as %systemroot% or %inetpub%. Full physical locations must be used.
- **Search for application on local system:** *(Optional)* Select if the application launcher should search the jump server or the calling workstation's file system for the executable being launched, and launch the first valid application it comes across. If this option is deselected, the **Application location** field becomes active, and a static path can be defined. Using search adds time needed to launch the application. The locations that can be searched are the Program Files directories or the system root directory. Searching is controlled by the subsequent options.



  - **Search for application on local system root** directs searches to the **%systemroot%** location on the jump server or the calling workstation's file system when launching an application.
  - **Search for application under the program files directory** directs searches to **%ProgramFiles%** and **%ProgramFiles (x86)%** on the jump server or the calling workstation's file system when launching an application.
  - **Subdirectory restriction** indicates the directories to not search when searching the Program Files directory structure.
  - **Additional search directories** are the additional directories to search if there are any other directories on the system to search. The list is semicolon delimited.
  - **Working Directory** is the default search starting point.

- **Only run signed executables:** *(Optional)* Select to ensure the program has a digital signature on it. If the option is enabled, an additional verification can be configured to validate specific fields of the digital signature, such as the certificate serial number, certificate issuer, etc.
  - **Verify certificate fields of signing certificate:** This option becomes available if **Only run signed executables** is selected. The resulting dialog allows definition around which fields to verify in the signing certificate.
- **Only run executables with expected hashes:** *(Optional)* Select if admins should be allowed to define hashes of a target application. This is useful to ensure a malicious executable is not renamed or a specific patched version has run. From this dialog, multiple hashes can be calculated and defined.

- **At launch, download the file from path:** *(Optional)* Define a network path or URL to download the application from if not already present on the host system.
- **Settings apply to client system configuration:** *(Optional)* Select if applications are launched from the user's workstation. This has no effect on applications launched using the jump server.
    - A 32-bit application running on a 32-bit Windows host installs to **c:\ProgramFiles\application**. Yet, the same 32-bit application running on a 64-bit Windows host installs to **c:\ProgramFiles (x86)\application**. This setting permits configuration of only one application to launch with multiple possible settings. When these settings are configured, the launcher determines which host it is running and retrieves the appropriate settings.
- **Application uses stored private key:** *(Optional)* Select this option to allow programs using certificates to define which certificate to use when connecting. These certificates must be pre-imported and assigned via the management console by choosing **Settings > User Keys > Import Keys**.
- **Application uses gateway server:** *(Optional)* If an SSH proxy/gateway is defined in the management console, this option is available. Select this option if a client should first connect to an SSH proxy before connecting to the final SSH target. This process uses **plink.exe**. The **plink.exe** download location must also be specified with the path on the jump server where the **plink.exe** executable is located. **Plink.exe** is installed in the launch app folder on the jump server if the PuTTy files are also installed. **Plink.exe** can also be downloaded from https://www.putty.org.
- **Configure Allowable Types:** *(Required)* Select which account types in the application are available. One account type, at minimum, must be selected. This option makes applications available to MySQL or Windows but not Linux, SQL Server, or Oracle.
- **Always use the specified account when starting this application:** *(Optional)* Select this option to pull a predefined credential from the account store and always use this account to launch the application. The application will not be available in the **Launch App** section of the web application. It will instead be made available in the **Applications** section of the website. **Applications** is always available regardless of managed passwords. When this option is NOT selected, the application is available for the selected account types. Potentially any account could be used to launch this application.

Variables for App Launching

Privileged Identity provides variables to pass the username, password, target server, etc., when launching an application from the command line or web automation scripts.

Scenario:

1. **DEMO\Broberts** logs into the web application.
2. **DEMO\Broberts** clicks on **launch app**, causing a secondary account, **DEMO\AppLaunchLogin**, to connect to the jump server. This action initiates and launches the **liebsoftlauncher.exe** program.
3. **Liebsoftlauncher** connects back to the web service and retrieves program settings, including target system, target user name, and target password. This connects him to a server called **DB2012** as **SA** with the **SA password**.

The following elements are defined using the following variables:

- **DEMO\Broberts = $(SourceAppLogin) or $(UserEnteredLoginUsername)**
- **DEMO\AppLaunchLogin = NOT EXPOSED**
- **DB2012 = $(RemoteAccessTarget_TargetName)**
- **SA = $(Username) or $(AccountName_FullyQualified)**
- **SA Password = $(Password) or $(Password_Raw)**

Following is a list of all possible variables:

- **$(UserEnteredLoginUsername):** Same as **$(SourceAppLogin)**, the account used to log in to the web application.
- **$(UserEnteredLoginUsername:RemoveNTStyleNamespace):** This element prunes the domain name from the user name. From the example above, DEMO\Broberts becomes simply Broberts.
- **$(UserEnteredLoginUsername:ReplaceBackslashWithDot):** This element retains the domain name with the username but replaces the slash with a dot. From the example above, DEMO\Broberts becomes DEMO.Broberts. Use this variable when a name is required that will not be interpreted as a path for creating directories.
- **$(SourceAppLogin)** - Same as **$(UserEnteredLoginUsername)**, the account used to log into the app triggering the launcher.
- **$(Username):** This is the name of the target account. From the example above, SA.
- **$(AccountName_FullyQualified):** Building on the **$(Username)** variable, this will pre-pend the domain prefix to the account name, if applicable.
- **$(Password):** The regex-escaped password (for example, pass\"word).
- **$(Password_Raw):** The raw, un-escaped password.
- **$(RemoteAccessTarget_TargetName):** The target host which the application connects to.
- **$(LauncherPath):** The path to the application launcher.
- **$(SessionID):** The GUID for the launcher link.
- **$(PrivateKey):** The file path for the DER encoded private key (if available).
- **$(PrivateKeyPassphrase):** The pass phrase, if present for **$(PrivateKey)**.
- **$(PuttyKey):** The file path for the PuTTY-encoded private key (if available).

These variables are used in line and are replaced by Privileged Identity when the application is launched. For example, if the user goes to the SQL Server database instance on a server called DB2012 and connects with the built-in (and managed) SA account from the website, the command line syntax would be:

```
-S $(RemoteAccessTarget_TargetName) -U $(Username) -P $(Password) - nosplash
```

The switches (-S, -U, and -P) are part of the **SMSS.EXE** executable. The subsequent values of **$(RemoteAccessTarget_TargetName)**, **$(Username)**, and **$(Password)** would be replaced by the name of the server (DB2012), the name of the account (SA), and the password for SA respectively.

Maintain Application Launching Scripts

As a courtesy to our customers, updated scripts that support common online business applications are periodically made available. This section describes how to download and install those files, and keep the script directory in sync across multiple launchers if script updates are required.

Install New Application Launching Scripts

1. Updated scripts area available with the installer at **%ProgramFiles (x86)%\Lieberman\Roulette\LaunchApp\WebAutomation**.
2. Customize the scripts as needed and test. Scripts are generic and may need to be customized to work in your environment.
3. Copy updated and customized automation scripts to the **WebAutomation** location. Be sure to also copy scripts to any secondary launchers.

> ***Note:*** *Third- party entities such as Facebook and Twitter change their variable requirements often and without warning. Scripts referencing third-party applications may need to be updated frequently.*

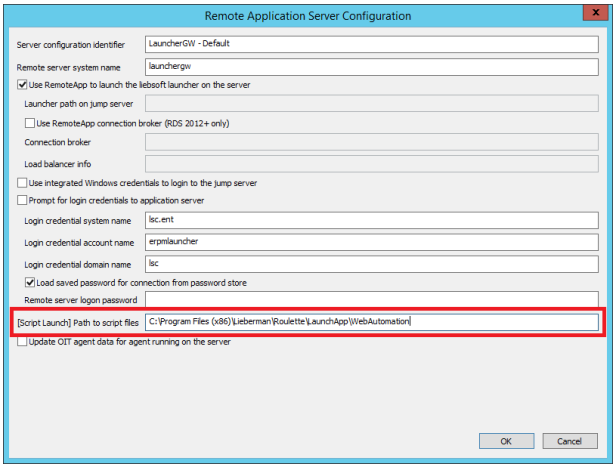
The following table lists the default file installation locations.

Application Launcher File(s)	Default installation location
Application launcher files to be installed on a bastion host, **LiebSoftLauncher.exe**	**%ProgramFiles(x86)%\Lieberman\Roulette\LaunchApp**
The automation scripts	**%ProgramFile (x86)%\Lieberman\Roulette\LaunchApp\WebAutomation**

> ***Note:*** *If you add your own compiled scripts to the **WebAutomation** folder, the defined login account must be able to read and execute the scripts.*

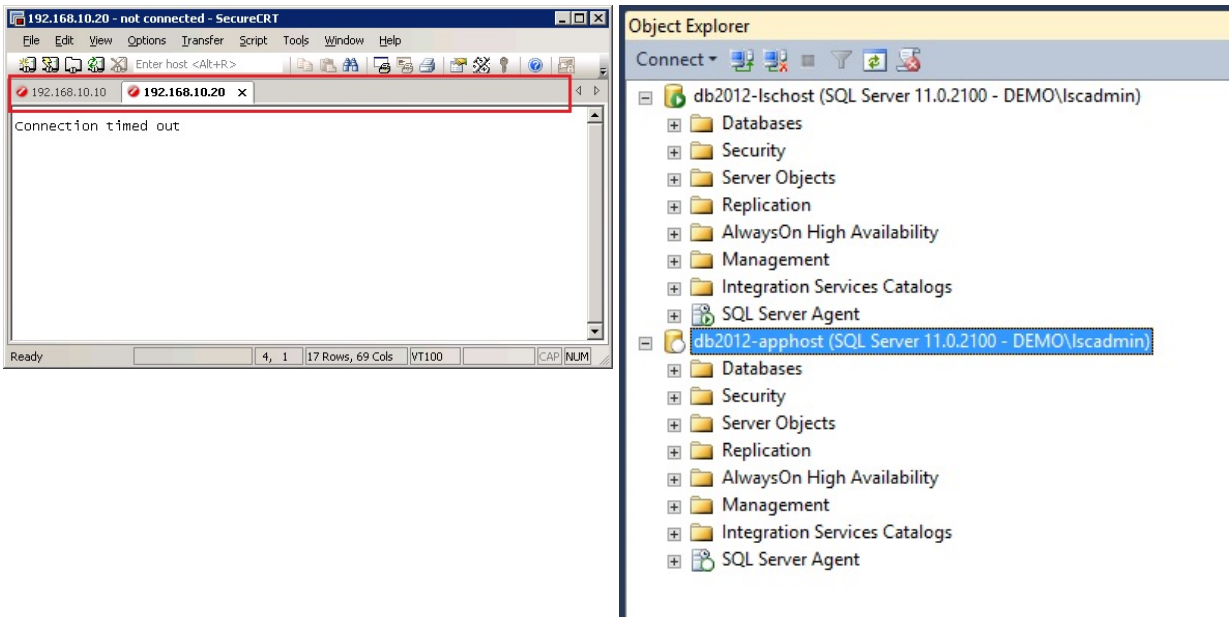
Verify the Script Launch Path Configured on Your Remote Application Server

1. In the management console, choose **Settings > Manage Web Application > Application Launch**.
2. Click **Remote Servers**.
3. Select the remote application server. Click **Edit**.
4. Refer to the **[Script Launch] Path to script files field** to view the path.



Multi-Tab Support

From one window, several administrative tools support connections to target systems. You can view multiple connections in separate tabs (like in SecureCRT) or like branches in tree-view navigation pane (like in Microsoft SQL Management Studio).



These applications can use different credentials for each target system connection. However, some applications have limitations when using multiple tabs or branches. For example, it is possible to use **Integrated Windows Authentication** to connect SQL Management Studio to some MS SQL servers, while others require an explicit SQL account using SQL authentication. In the case of SQL Management Studio, when the tool is launched and integrated, Windows authentication is used, and it is not possible to reuse the existing instantiation of the tool. However, if one connection uses integrated authentication and the secondary connections use SQL authentication, or if all connections use SQL authentication, you can reuse the currently running instance.

Privileged Identity supports this functionality via the **Multi-tab Configuration** window in **Remote Application Configuration**.

If multi-tab is not used, when a user launches a tool like SecureCRT or SQL Management Studio, it establishes one session on the jump server and one instance of the application in that session. This is a more secure scenario because it segregates the data and session information so it cannot be shared within the tool or within any systems the user may be accessing.

The trade-off is that a secondary launch of the same tool, just to a new system, will cause a second session to be created, and it can be slow and consume more resources.

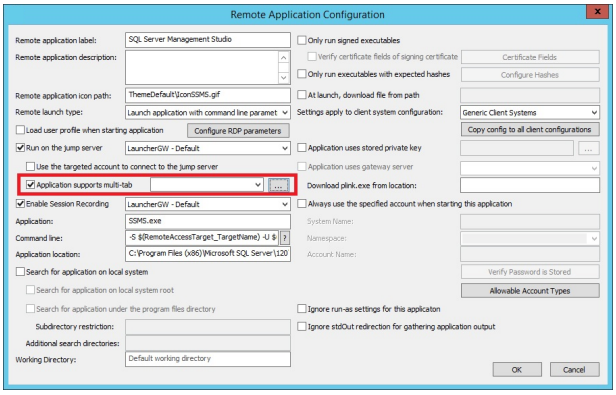
If multi-tab is used, when a user launches a tool such as SecureCRT or SQL Management Studio, it establishes one session on the jump server and one instance of the application in that session. Then, when a user launches the same tool again to connect to another system, it reuses the existing session and adds a tab or another tree to the tool. This reduces resource consumption on the jump server and can speed up the use of the tool. The trade-off is that the application can share information from all servers with anything it is connected to.

Configure Multi-Tab Support

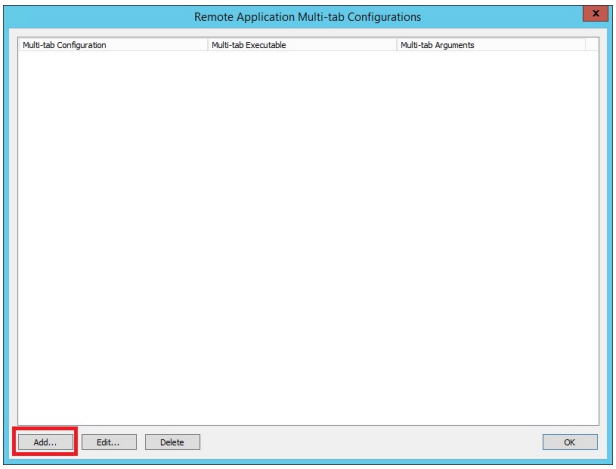
To configure multi-tab support, make sure the jump server and basic application settings have been set up.

> ***Note:*** *Mutli-tab is supported for application launching from a jump server only.*

1. From **Remote Application Configuration**, enable the **Application supports multi-tab** option . Click the **...** button.



2. Click **Add**.



3. Complete all the information on the **Multi-tab Configuration** dialog.
   - **Multi-tab configuration label** is a label shown in the **Multi-tab Configuration** selection in the **Remote Application Configuration** window.
   - **Multi-tab automation local executable path** is a path to a compiled AutoIT script, which is able to open a new tab or establish a connection to new target system.
   - **Automation executable arguments** are specific to new-tab-executables. The ProcessID is used to find the handle of the application window, and the target system is transferred to the application for a new connection. Username and password are not needed.
   - **Allow this multi-tab automation for existing application launches by EXE name** controls how launched applications are detected. If it is unchecked, the applications selected from the multi-tab configuration are assumed to be previously launched.

In the example, we are using SQL Management Studio. There are two different application configurations: one for Integrated Windows Authentication and another one for SQL server authentication. Both scenarios use the same executable, **ssms.exe**. For

Integrated Windows Authentication where different Windows accounts are being used to connect to target database servers, the option to **Allow this multi-tab automation for existing application launches by EXE name** should be unchecked. While using integrated Windows authentication and the SSMS process was launched from another user, it is impossible to connect to a secondary instance of MS SQL using the existing instance of **smss.exe**. The automation executable arguments should be similar to:

```
$(RemoteAccessTarget_TargetName) nouser nopasswords $(ProcessID)
```

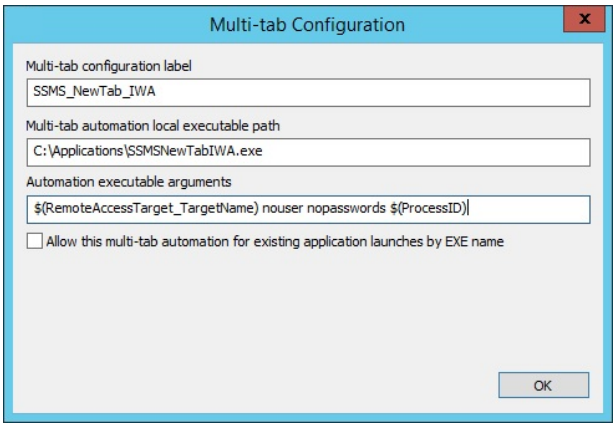
ProcessID is the ID utilized to reuse the currently running executable.

For SQL Management Studio where SQL Authentication is being used, the option to **Allow this multi-tab automation for existing application launches by EXE name** can be selected. The automation executable arguments should be similar to...

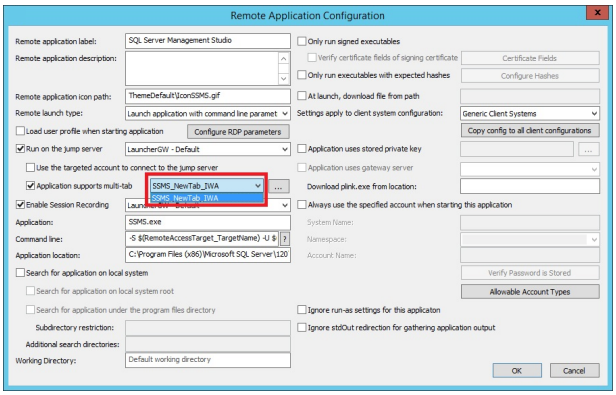
```
-S $(RemoteAccessTarget_TargetName) -U $(Username) - P $(Password_Raw)
```

In the commands above, **$(RemoteAccessTargget_TargetName)**, **$(Username)**, and **$(Password_Raw)** are standard variables. **$(ProcessID)** is a variable that returns the PID of the initial launched application. The **nouser** and **nopasswwords** values are for username and passwords arguments. Because we use Integrated Windows Authentication, we do not need user name and password arguments.

SSMSNewTablwa.exe and **SSMSNewTabSql.exe** are compiled AutoIT scripts that we use to interact with Microsoft SQL Server to open new connections that use Integrated Windows Authentication or SQL authentication.



Click **OK**. Select the appropriate multi-tab configuration settings for the target application.



Multi-tab scripts have been compiled for the following applications:

- **RunAs and wait until process finishes** = RunAsWait
- **DHCP Manager** = RunDHCP
- **DHCP Manager** = RunDHCPNewTab
- **DNS Manager** = RunDNS
- **DNS Manager** = RunDNSNewTab
- **File Server Resource Manager** = RunFSRM
- **Hyper-V Manager** = RunHyperV
- **Hyper-V Manager** = RunHyperVNewTab
- **MS Terminal Services** = RunMstsc
- **Network File Services Management** = RunNFSMGMT
- **Performance Monitor** = RunPERFMON
- **Server Manager** = RunServerManager

- **Storage Explorer** = RunStorageExplorer
- **Storage Manager** = RunStorageMgmt
- **Task Scheduler** = RunTaskScheduler
- **Run process and wait until finished** = RunWait
- **WBAdmin (Backup)** = RunWBADMIN
- **WINS Manager** = RunWINS
- **WINS Manager** = RunWINSNewTab
- **SecureCRT** = ARM_SCRTStart
- **SecureCRT** = SCRTNewTabSSH2
- **SecureCRT** = SCRTNewTabTELNET
- **SecureCRT** = SCRTStart
- **SQL Mgmt Studio** = SSMSNewTabIwa
- **SQL Mgmt Studio** = SSMSNewTabSql
- **A simple test script** = TestParams
- **Remote Desktop** = UnlockMstsc
- **Remote Desktop for ARM** = UnlockMstscARM

Multi-Tab AutoIT Script Examples

SSMSNewTabIwa.au3

```
#include <MsgBoxConstants.au3>
local $paramCount = $CmdLine[0]
local $systemName = $CmdLine[1]
local $domainUserName = $CmdLine[2]
local $password = $CmdLine[3]
local $ssmsPid = $CmdLine[4]
if $paramCount = 4 Then
      openNewTab($ssmsPid, $systemName, $domainUserName, $password)
EndIf
Func openNewTab($p_ssmsPid, $p_systemName, $p_domainUserName, $p_password)
      Opt("WinTitleMatchMode", 2)
      local $ssmsWindows = WinList("Microsoft SQL Server Management Studio")
      for $i=1 To $ssmsWindows[0][0]
            If $ssmsPid=WinGetProcess($ssmsWindows[$i][1]) Then
                  local $delay = 5
                  WinActivate($ssmsWindows[$i][1])
                  WinWaitActive($ssmsWindows[$i][1])
                  Send('!f')
                  Sleep($delay)
                  Send('e')
                  Sleep($delay)
                  Send('+{TAB}')
                  Sleep($delay)
                  Send('+d')
                  Sleep($delay)
                  Send('{TAB}')
                  Sleep($delay)
                  Send($systemName)
                  Sleep($delay)
                  Send('{TAB}')
                  Sleep($delay)
                  Send('+w')
                  Sleep($delay)
                  Send('{ENTER}')
            EndIf
```

```
      Next
EndFunc
```

SSMSNewTabSql.au3

```
#include <MsgBoxConstants.au3>
local $paramCount = $CmdLine[0]
local $systemName = $CmdLine[1]
local $domainUserName = $CmdLine[2]
local $password = $CmdLine[3]
local $ssmsPid = $CmdLine[4]
if $paramCount = 4 Then
      openNewTab($ssmsPid, $systemName, $domainUserName, $password)
EndIf
Func openNewTab($p_ssmsPid, $p_systemName, $p_domainUserName, $p_password)
      Opt("WinTitleMatchMode", 2)
      local $ssmsWindows = WinList("Microsoft SQL Server Management Studio")
      for $i=1 To $ssmsWindows[0][0]
            If $ssmsPid=WinGetProcess($ssmsWindows[$i][1]) Then
                  local $delay = 5
                  WinActivate($ssmsWindows[$i][1])
                  WinWaitActive($ssmsWindows[$i][1])
                  Send('!f')
                  Sleep($delay)
                  Send('e')
                  Sleep($delay)
                  Send('+{TAB}')
                  Sleep($delay)
                  Send('+d')
                  Sleep($delay)
                  Send('{TAB}')
                  Sleep($delay)
                  Send($systemName)
                  Sleep($delay)
                  Send('{TAB}')
                  Sleep($delay)
                  Send('+s')
                  Sleep($delay)
                  Send('{TAB}')
```

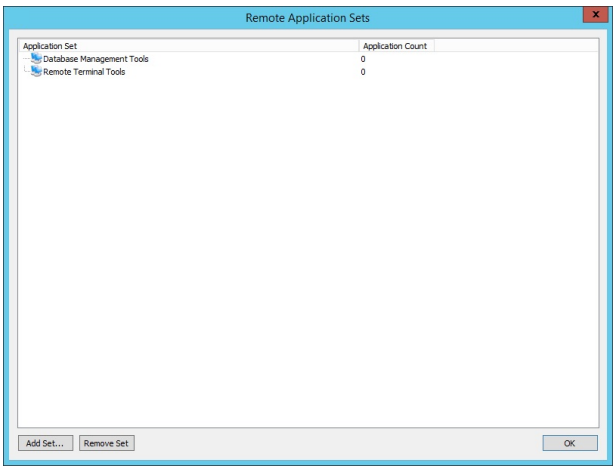
```
                Sleep($delay)
                Send($domainUserName)
                Sleep($delay)
                Send('{TAB}')
                Sleep($delay)
                Send($password)
                Sleep($delay)
                Send('{ENTER}')
            EndIf
        Next
EndFunc
```

Configure Application Sets

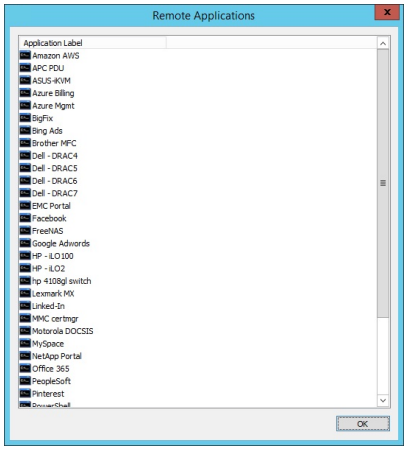
Application sets are pre-defined collections of applications to launch.

Create an Application Set

1. Open the management console.
2. Go to **Settings > Manage Web Application > Application Launch**.
3. Click **App Sets > Applications**.
4. Click **Add Set**.
5. Enter a name and click **OK**.

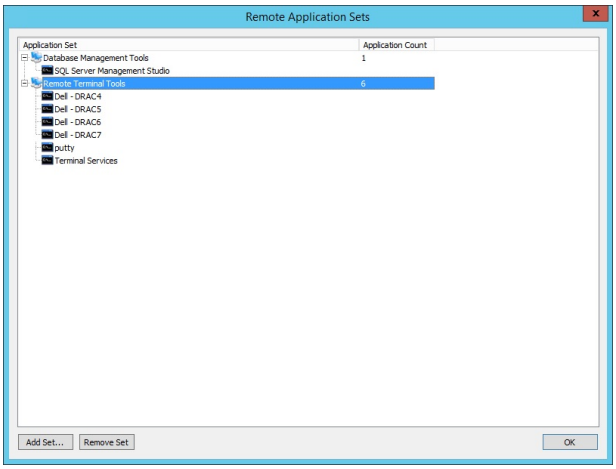


6. To add applications to the application set, right-click the application set.
7. Select **Add applications to set**.
8. Select all the desired applications and click **OK**.



9. To view the applications added to an application set, expand the application set.

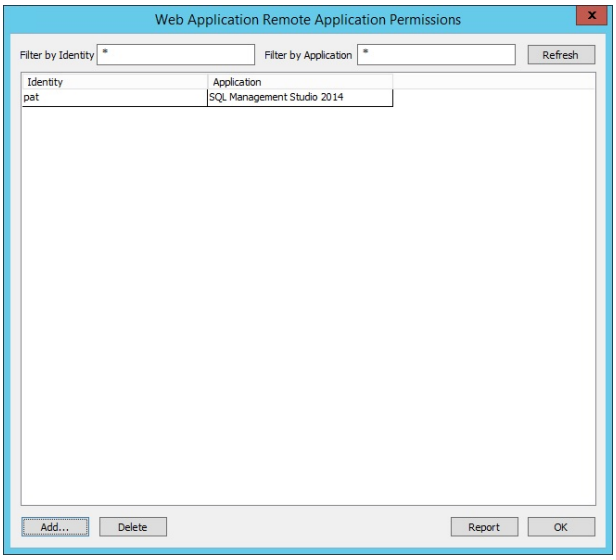
Once application sets are defined, users who do not have **All Access** must have application set permissions and application permissions set.



Define Application Permissions

When a user does not have **All Access** privileges, additional permissions are required to launch a specific application. Use the management console to define these permissions.

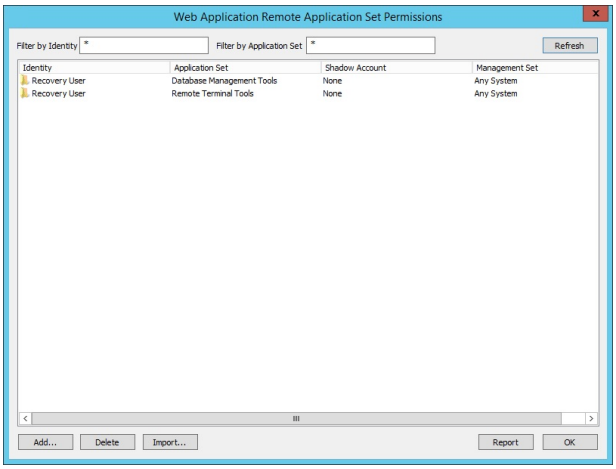
1. Open the management console.
2. Choose **Delegation > Web Application Remote Application Permissions**.
3. Click **Add**.
4. Select an available identity and click **OK**. Select one or more applications the user can launch.



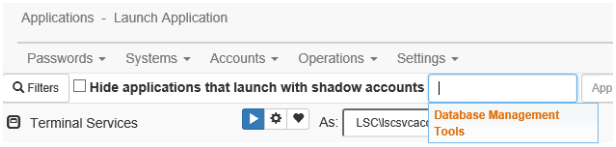
Define Application Set Permissions

1. Open the management console.
2. Choose **Delegation > Web application Remote Application Set Permissions**.
3. Click the **Add**.
4. Click **OK**.
5. Select from the available application sets and click **OK**.
6. If a **Shadow Account** is used, click **Yes**. Enter the required information. Otherwise, click **No**.

7. If there are system restrictions, click **Yes**. Enter the required information. Otherwise, click **No**.



8. Select the applications users are able to launch from the website.



Set Up Shadow Accounts

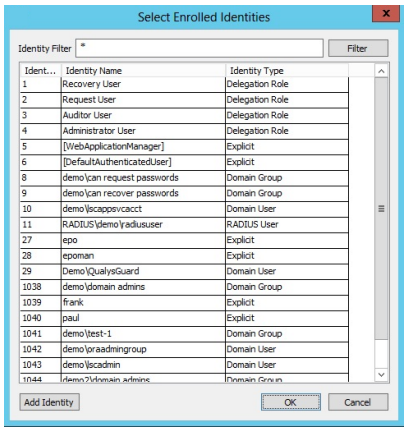
Shadow accounts allow users to connect to a system with a specific application and choose which account to connect with. The normal paradigm requires users to go the **Managed Passwords** section and find the target system and local account for the application. While this works for many scenarios, it is not very flexible, and it does not address the need be able to connect domain or directory accounts to other systems or applications.

With a shadow account, users can go to the system or application in the **Systems View** of the web application and choose to launch an application. A list of applications is presented, and users can determine which account, local or central (domain or directory), to connect with.

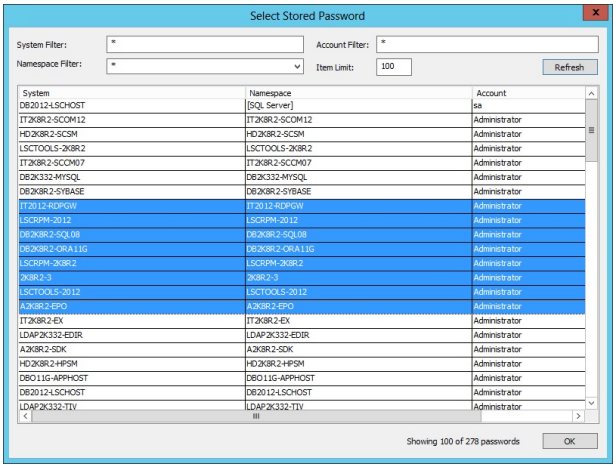
To use shadow accounts, the **View Systems** and **Allow Remote Sessions** global delegation permissions must be assigned. Once permissions are granted, additional configuration to map shadow accounts must be performed.

Even when users have **All Access** privileges, shadow accounts are first mapped and associated with application permissions. To use shadow accounts, a per-application rule must be established for the target user. Follow the steps below to add a new shadow account mapping.

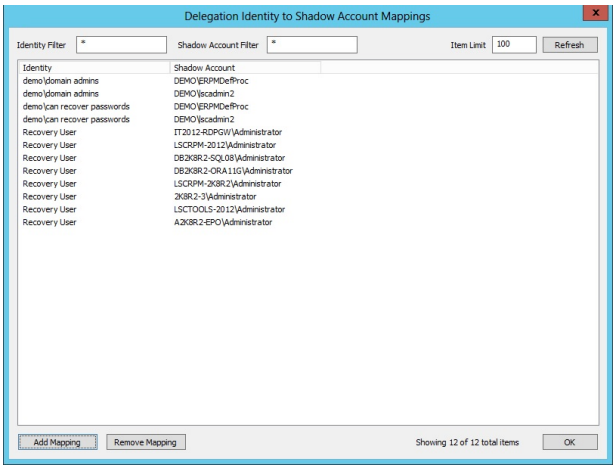
1. Open the management console.
2. Go to **Delegation > Web Application Identity to Shadow Account Mappings**.
3. Click **Add Mapping**.



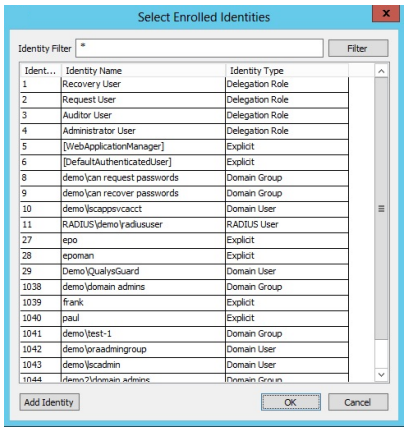
4. Select the target identity from the list of available identities. Click **OK**.



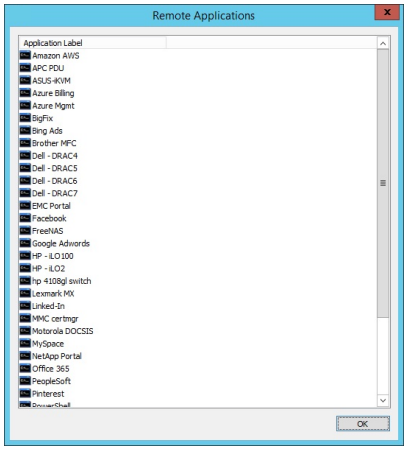
5. Select from the available managed/stored identities and click **OK**. The new mappings will now be in the list of available mappings.
6. Click **OK**.
7. Go to **Delegation > Web Application Remote Application Permissions**.



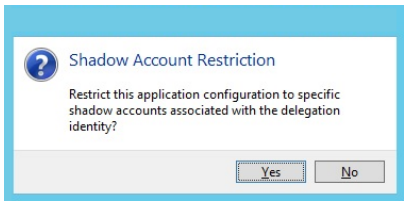
8. Click **Add** in the lower left corner of the **Remote Application Permissions** dialog to add a new application permission. Select the identity and click **OK**.



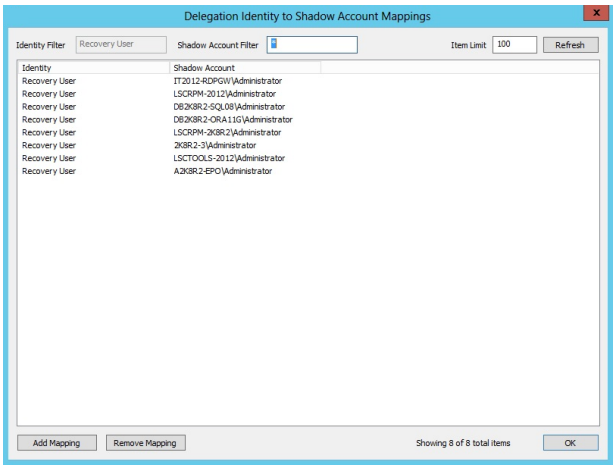
9. A list of remote applications will be presented. Select the target application to make available. Click **OK**.



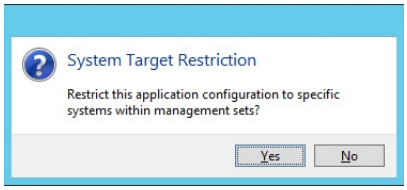
10. A **Shadow Account Restriction** prompt appears. Click **Yes** to assign one or more shadow accounts the user may use when launching the specified application.



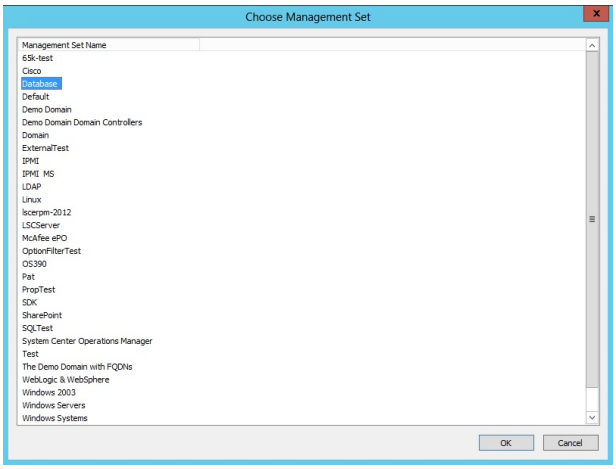
11. Based on the selected user, a list of available corresponding mappings is presented. Select the mapping configured for the target user and selected applications. Click **OK**.



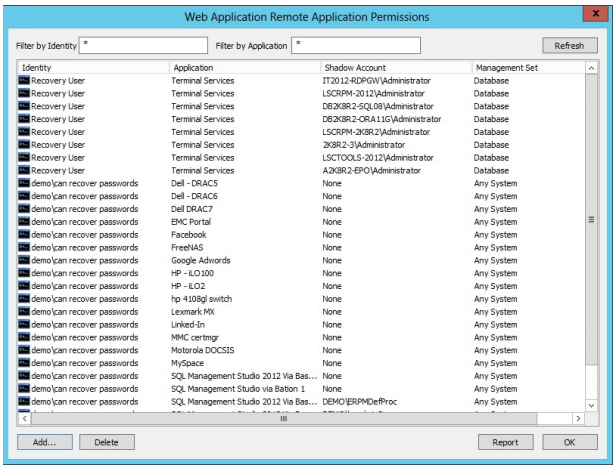
12. A **System Target Restriction** prompt appears. If it is desired to restrict the applications and or shadow account mappings to specific list of systems, click **Yes**. Otherwise, click **No**.



13. If **Yes** is selected, a list of management sets are presented.



14. Select the desired management set and click **OK**.
15. The new mapping is presented in the **Web Application Remote Application Permissions** dialog. Any undesired mappings may be deleted. Reports may be generated from this page.



16. To use the mappings, the user must go to the **Systems View** in the web application.

17. Click **Launch App** next to the desired target system. If **Launch App** is not visible, it means the user does not have either the **Allow Remote Sessions permission**, or a **Shadow Account Mapping** is not present.

Set User Permissions to Launch Applications and Use the Application Launcher

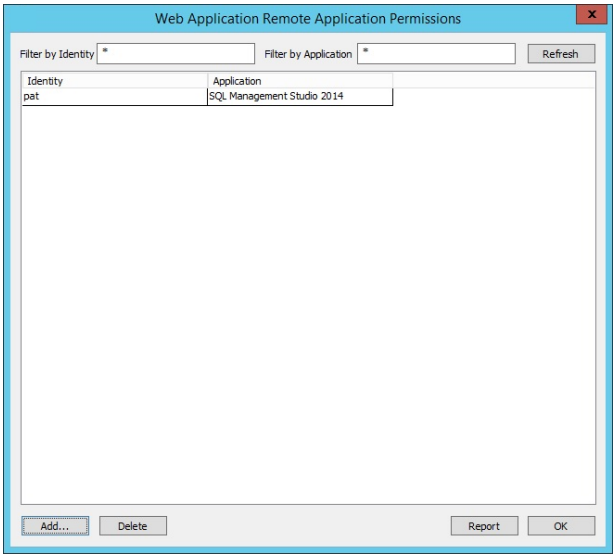
To launch an application a user must have one of the following sets of permissions:

- **All Access**
- Or **View Accounts, Allow Remote Sessions**, and permissions for the specific application being launched

Set Permission to Launch Applications

To define the additional permissions required to launch a specific application, follow the steps below.

1. Open the management console.
2. Choose **Delegation > Web application remote application permissions**.
3. Click **Add**.
4. Click **OK**.
5. Select one or more applications the user can launch.

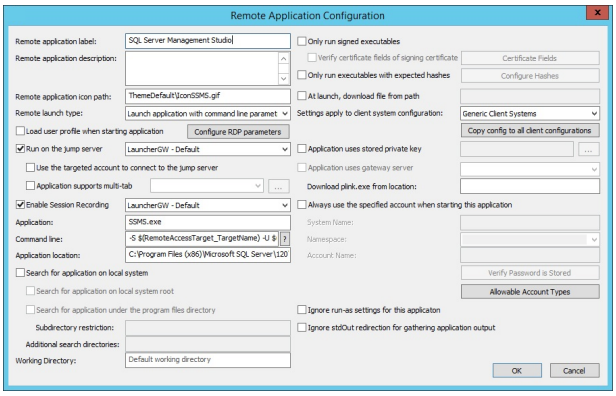


Use the Application Launcher

There are two types of application launching in Privileged Identity:

- Launching with a variable account and system information
- Launching with a predefined account and system information

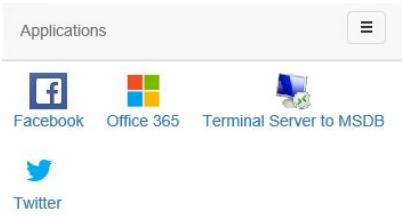
If the **Always use the specified account** option is selected, the application appears in the **Applications** section of the website. If the option is not selected, the user must go to the **Launch App** section to connect.



Launch an App as a Pre-Configured Application

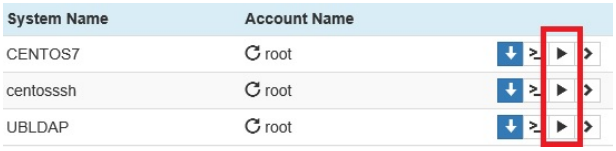
To launch an application pre-configured for a specific account and target, click **Operations > Applications** and select the application to launch. Only applications that are pre-configured to always launch as a specific user are displayed. If an application is not shown, it is a sign of at least one of two possible causes:

- The user does not have permission to launch an application.
- There are no apps configured to always run as a specific user.



Launch an App Using Variable Target and Account Information

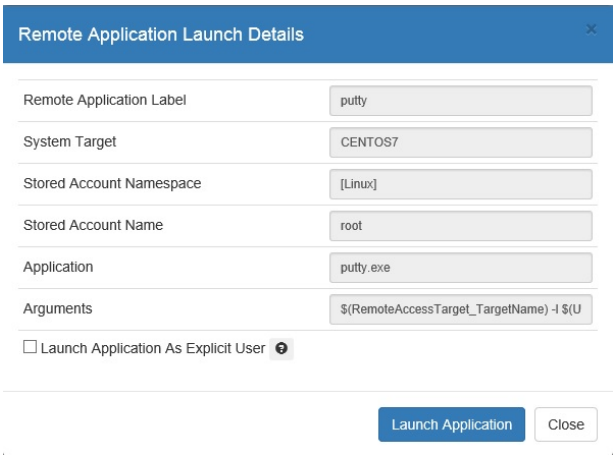
Once the the target system and account are located in the **Passwords > Managed Password** section of the website, click the **Play** button.



All applications available to the user for the specific account type are shown. Use the filter options at the top of the page to search for applications, show only a set of applications, or change the layout of application launcher page. If the RDP icon appears, the application is configured to launch via the jump server. If the camera icon appears, the session will be recorded.

To launch the application, click **Launch**. The order of events will vary depending on whether the application is configured to launch locally or from a jump server and whether the user has previously performed this process or not. If connecting via a jump server, the system initiates a series of calls to the jump server and the **LiebsoftLauncher** on that host. This will be visible to the user. If the user has not previously launched an app from the machine/profile that they are currently logged into, they receive a couple of security prompts

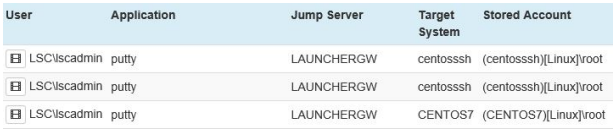
Each application also has an **Advanced** launch configuration. Click the ear icon to allow the user to specify alternate credentials to connect to the target system. These could be static credentials or other stored credentials in Privileged Identity.



Audit Recorded Sessions

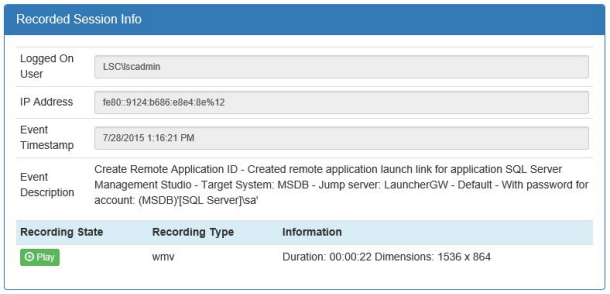
Once sessions have been recorded, users with access to the **Auditing** section of the web application are able to play back any recorded sessions. Recorded sessions will have camera icons next to their audit entries.

Click on the camera icon to playback the recorded sessions.

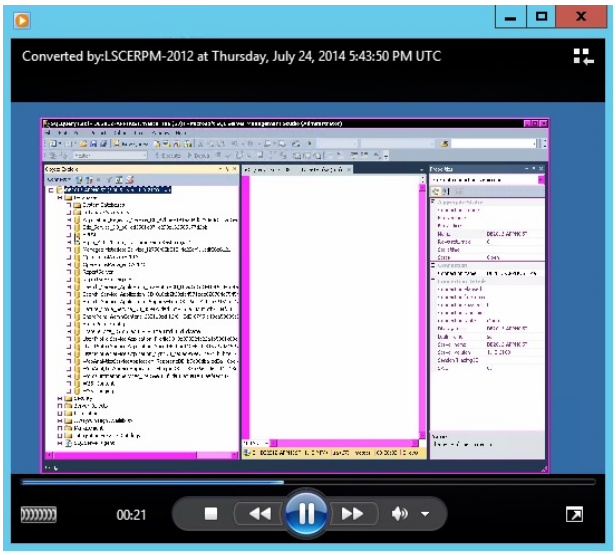


User	Application	Jump Server	Target System	Stored Account
LSC\lscadmin	putty	LAUNCHERGW	centosssh	(centosssh)[Linux]\root
LSC\lscadmin	putty	LAUNCHERGW	centosssh	(centosssh)[Linux]\root
LSC\lscadmin	putty	LAUNCHERGW	CENTOS7	(CENTOS7)[Linux]\root

The session properties page displays the **Logged On User**, **IP Address**, **Timestamp**, and **Event Description**. To play back the recording, choose the desired recording and click **Play**.



The video will open on the system's preferred media player and begin streaming automatically.



Upgrade the Application Launcher and the Session Recording Software

Follow the steps below to upgrade the application launcher and session recording for Privileged Identity.

1. Upgrade Privileged Identity, the web application, and web service.
2. Make note of the web service URI. It is required for the application launcher and session recording to work properly.
3. Re-run the application launcher and session recording installer on all host servers. Most of your settings will be remembered. However, during session recording installation, you must enter your service account credentials when prompted.

Note: *You will not need to restore previously configured applications or application settings.*