Citrix Session Remote Start

Contents

Introduction

January 16, 2025

For organizations using virtual apps and desktops, productivity starts after logging in. However, prolonged logon times, often lasting several minutes, disrupt workflows and disappoint the employees. Citrix Session Remote Start addresses this challenge by delivering seamless, efficient, and faster access to virtualized resources.

Session Remote Start provides APIs for trusted third-party services to enumerate, launch, and log off Citrix sessions. It enables unattended logons triggered by events like building badge scans, eliminating delays in time-intensive environments. Optional logon scripts can disconnect sessions post-logon, keeping them ready for users to reconnect when needed.

With seamless integration into existing Citrix components, Session Remote Start simplifies deployment, enhances user experiences, and redefines how businesses manage virtualized access boosting the overall productivity.

System Requirements

The following table lists the minimum requirements for a Session Remote Start server.

Requirements	Details
OS	Windows Server OS - recommended 2019 and above
Processor	4 or more cores on a compatible 64-bit processor with 2 GHz or faster
RAM	Min 16GB
Storage	50

Other component requirements

The Session Remote Start requires the following components:

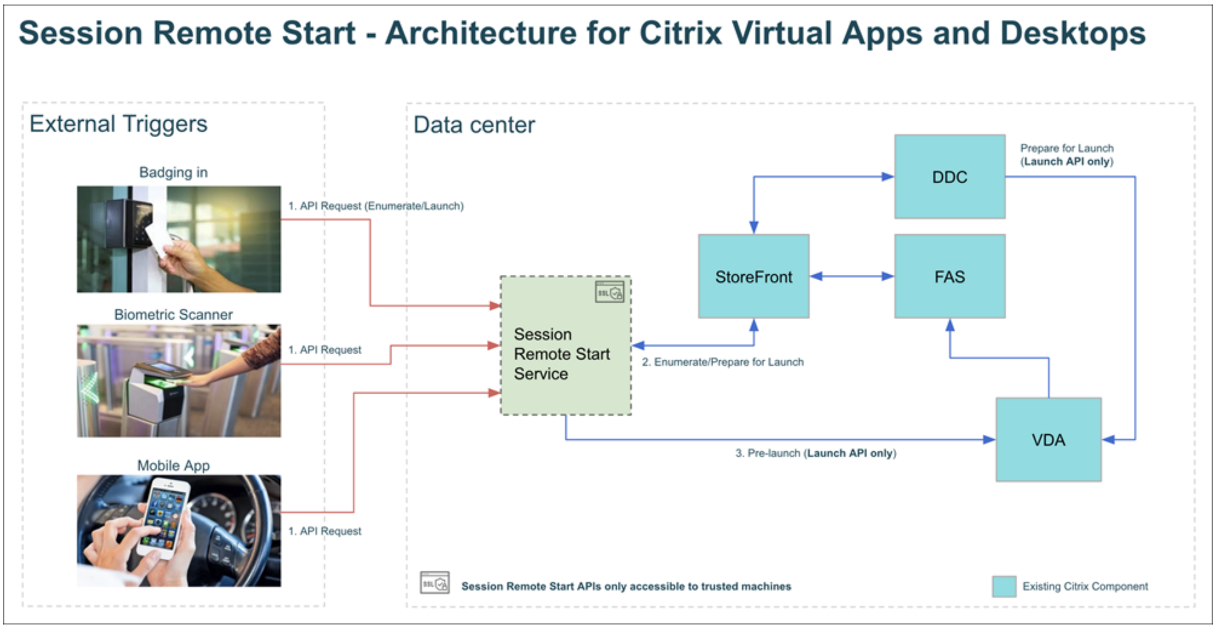
1. **Windows Active Directory (AD)** or Microsoft Entra hybrid-joined.
2. Citrix StoreFront 2203 and above.
3. Citrix FAS (Federated Authentication Service).
4. Session Remote Start must have direct line-of-sight to **Citrix StoreFront** (and vice versa) and VDAs intending to be pre-launched.

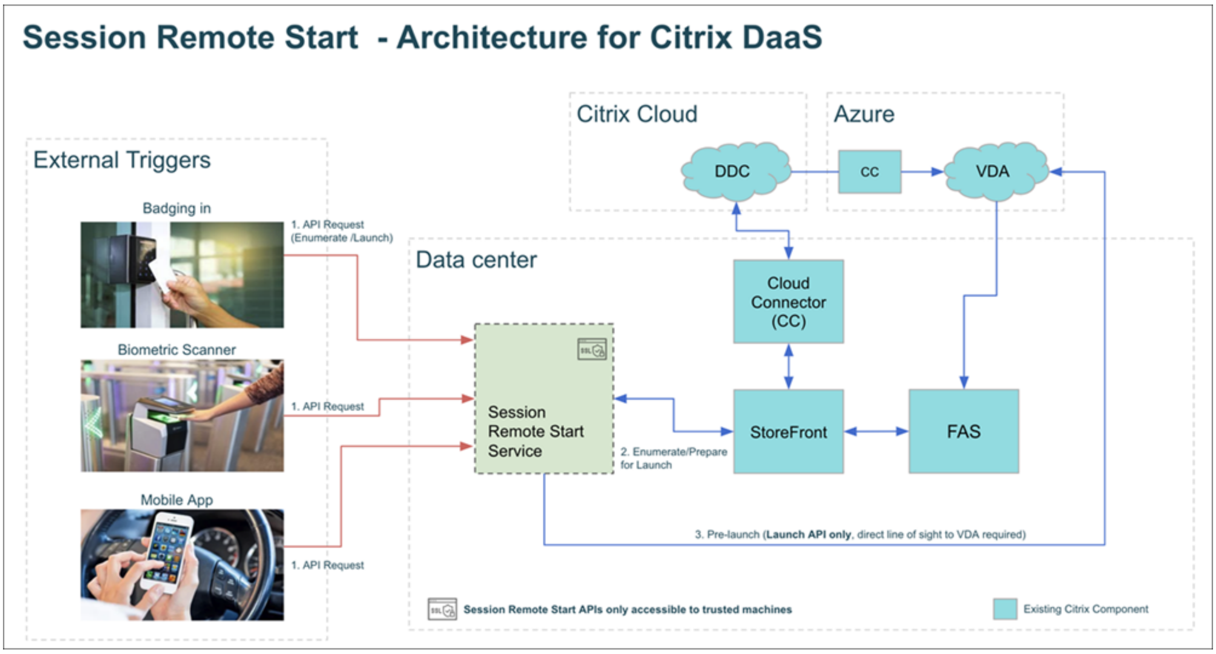
5. It is recommended that a **new store** is created within Citrix StoreFront for Session Remote Start usage, and Session Remote Start usage only.
6. **IIS is required** on the Session Remote Start server. If IIS is not installed already, Session Remote Start installs it.
7. **SSL Certificates** must be installed on both the Session Remote Start server and the servers making API requests.
    - This ensures that only trusted services can issue requests to Session Remote Start.
    - Installation of certificates must be performed by an admin after installation. This document guides you but the certificates must be provided by the customer.

> **Important Note:**
>
> Session Remote Start works with Citrix Virtual Apps and Desktops on-prem and Citrix DaaS when StoreFront is used. Currently, Session Remote Start does not work with Citrix Workspace (Cloud version of StoreFront). StoreFront is a requirement for Session Remote Start.

Architecture: Citrix Virtual Apps and Desktops and Citrix DaaS

You can deploy Session Remote Start on both Citrix Virtual Apps and Desktops and Citrix DaaS environments as long as you use Citrix StoreFront in DaaS instead of Citrix Workspace. Here are the high-level architecture diagrams that explain the data flow, user action, and Session Remote Start workflow.


Session Remote Start - Architecture for Citrix Virtual Apps and Desktops
External Triggers
Badging in
Biometric Scanner
Mobile App
1. API Request (Enumerate/Launch)
1. API Request
1. API Request
Data center
Session Remote Start Service
StoreFront
DDC
FAS
VDA
Prepare for Launch (Launch API only)
2. Enumerate/Prepare for Launch
3. Pre-launch (Launch API only)
Session Remote Start APIs only accessible to trusted machines
Existing Citrix Component


Session Remote Start - Architecture for Citrix DaaS
External Triggers
Badging in
Biometric Scanner
Mobile App
1. API Request (Enumerate /Launch)
1. API Request
1. API Request
Citrix Cloud
DDC
Azure
CC
VDA
Data center
Cloud Connector (CC)
Session Remote Start Service
2. Enumerate/Prepare for Launch
StoreFront
FAS
3. Pre-launch (Launch API only, direct line of sight to VDA required)
Session Remote Start APIs only accessible to trusted machines
Existing Citrix Component

Installation of Session Remote Start

January 16, 2025

Installation Steps

- Download the latest Session Remote Start installer from Citrix Downloads.
- Double-click `Citrix.Srs.Installer_x64.msi`.
- Be sure to install as an administrator and follow the on-screen instructions to complete the installation.

Alternatively, you can install Session Remote Start from command line and specify the log path (MSI installation log, not Session Remote Start runtime log):

```
.\Citrix.Srs.Installer_x64.msi /L*v out.log
```

Customers can run `.\Citrix.Srs.Installer_x64.msi /?` to get more install or uninstall options.

Certificates

January 15, 2025

Install SSL Certificate for Accessing StoreFront

Session Remote Start is hosted on IIS and runs under a different identity to the user installing the certificate. Ensure that the Session Remote Start service has permissions to load the certificate.

> **Note:**
>
> It is suggested to install the certificate under **Local Machine** so that all users can access it.

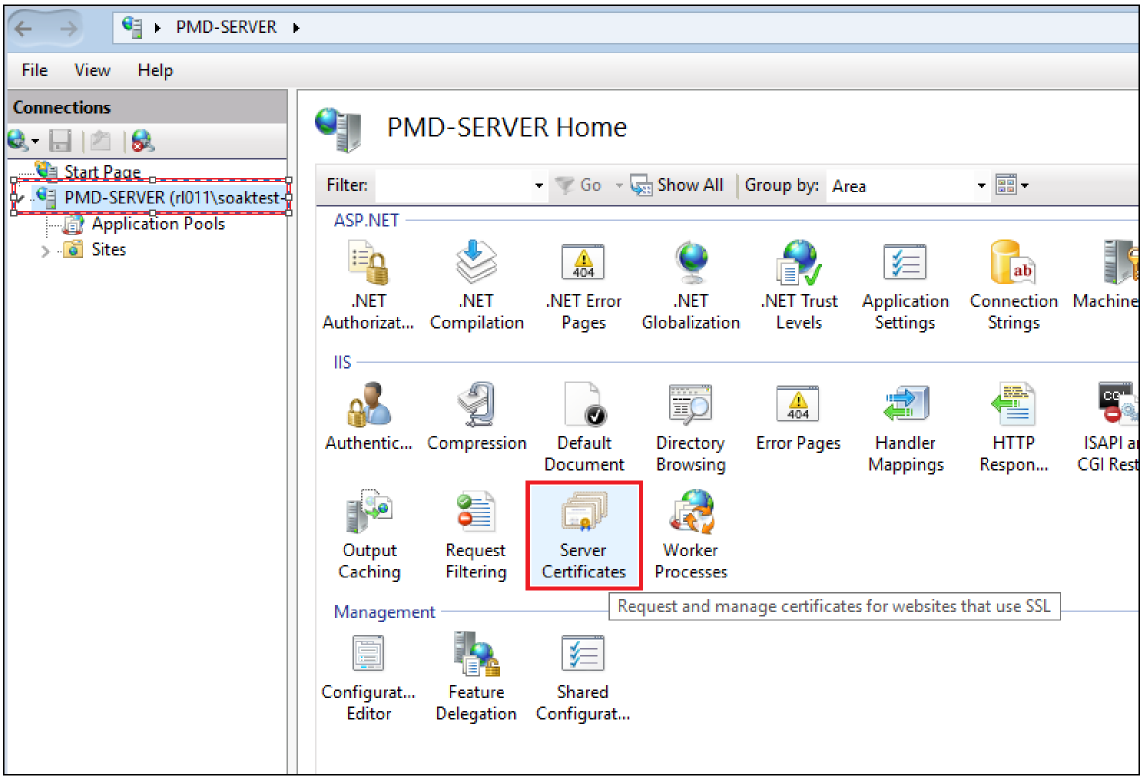
The **IIS identity** under which Session Remote Start is running must be able to visit the StoreFront URL of **Receiver for Web Site** without warning. (For example, `https://storefront.rl011.local/Citrix/srsWeb`)

Import Server SSL certificate to IIS Manager

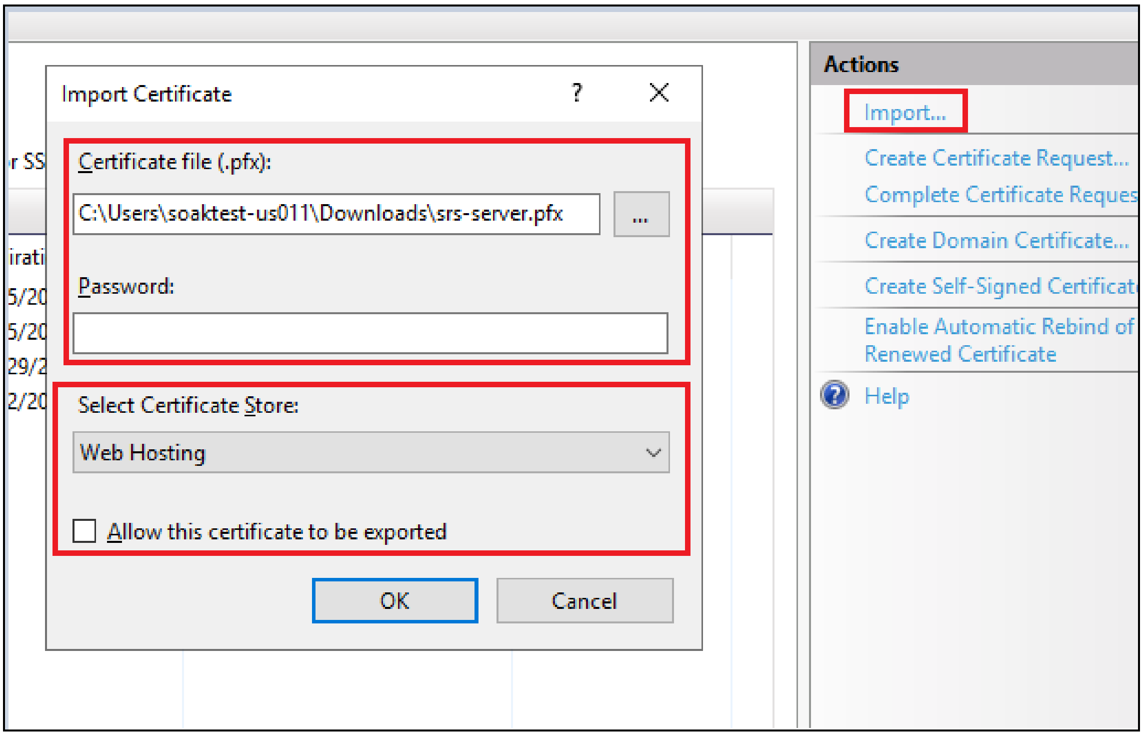
> **Note:**
>
> Skip this step if Session Remote Start is already configured and set as your default website.

Securing access and encrypting traffic with SSL certificates is the preferred way of deploying Session Remote Start. The secure access and encrypt traffic with SSL certificates:

1. Open up IIS Manager, select the Session Remote Start Server name, and open the **Server Certificates**.



2. Click **Import…** in the **Actions** panel on the right.



Import Certificate

Certificate file (.pfx): C:\Users\soaktest-us011\Downloads\srs-server.pfx

Password:

Select Certificate Store: Web Hosting

□ Allow this certificate to be exported

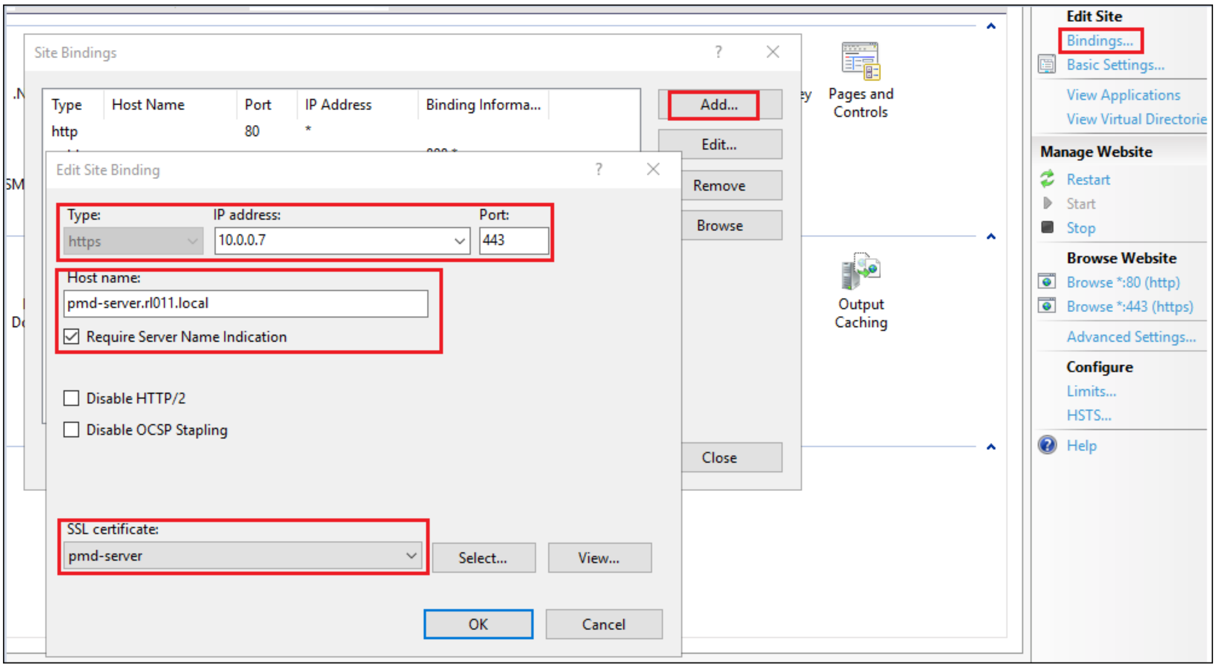
?
X
...
OK
Cancel
r SS
irati
5/20
5/20
29/2
2/20
Actions
Import...
Create Certificate Request...
Complete Certificate Reques
Create Domain Certificate...
Create Self-Signed Certificat
Enable Automatic Rebind of Renewed Certificate
Help

Make sure the Session Remote Start service IIS identity has the necessary permissions to load the certificate. The settings shown for **Certificate store** and **Allow this certificate to be exported** in the images are recommended for better security. If **Web Hosting** is selected, remember to import the full certificate chain.

Create HTTPS Binding

> **Note:**
>
> Skip this step if Session Remote Start is already configured and set as your default website.

Create an HTTPS binding in IIS Manager.



Site Bindings

Type	Host Name	Port	IP Address	Binding Informa...
http		80	*	

Edit Site Binding

Type: https

IP address: 10.0.0.7

Port: 443

Host name: pmd-server.rl011.local

☑ Require Server Name Indication

□ Disable HTTP/2

□ Disable OCSP Stapling

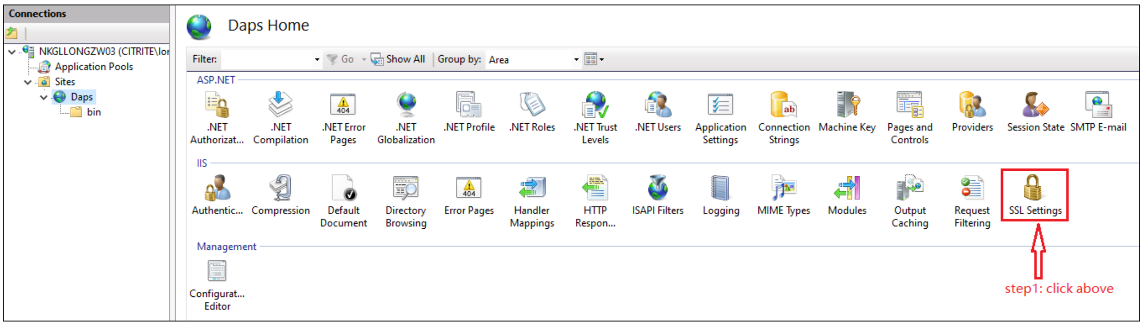
SSL certificate: pmd-server

1. On the IIS Manager, click **Default Web Site** under **Sites**. On the right panel, under **Actions > Edit Site**, click **Bindings**.
2. Click **Add**.
3. Under the **Add Site Binding** screen.
   - Select the type as **https**.
   - Set https port to **443**.
   - Enter the IP address and host name of Session Remote.
   - Start server respectively in the respective fields.
   - Click **OK**.
   - Now, click **Edit** on the newly created Binding.
   - Select the **SSL certificate**.

In this guide, for the **Binding** settings, we only consider that third-party Auth Service and StoreFront establish the same Session Remote Start endpoint (Network Interface). If not, we must remove the IP address and Hostname limitation and clear the **Require Server Name Indication** check box in the settings.

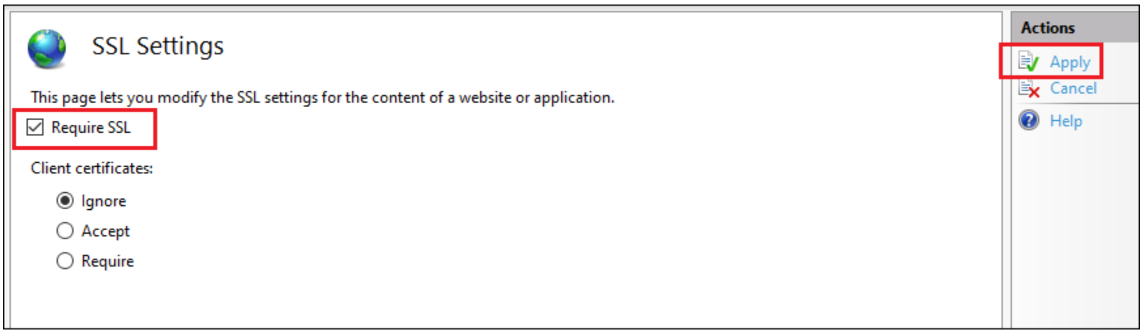
Require SSL

1. In IIS Manager, select the **Session Remote Start Site**, and double click **SSL Settings**.



step1: click above

2. On the SSL Settings page, check **Require SSL** and under **Client Certificates**, select **Ignore** and click **Apply**.



This page lets you modify the SSL settings for the content of a website or application.

☑ Require SSL

Client certificates:

● Ignore

○ Accept

○ Require

Configure Session Remote Start

January 15, 2025

Configuration file

Session Remote Start configuration parameters are stored in the **Web.config** file found under the Session Remote Start installation directory (`'C:\Program Files\Citrix\SessionRemoteStart\'` by default).

Parameter	Optional/Required	Description
StoreFrontServer	Required	The Web URL of the store explicitly created for Session Remote Start

Parameter	Optional/Required	Description
		`<add key=" StoreFrontServer" value="https://< baseURL>/Citrix/< storename>Web"/>`
RestAPIUrl	Optional	CVAD RestAPI URL For On-Prem should be `https://[ DdcServerAddress]`, For Citrix DaaS should be `https://api.cloud.com`
RestAPICredentialName	Optional	The credential created in previous section - `' CVAD_RestAPI_Credential 'by default.`
LocalFqdn	Required	FQDN of Session Remote Start server. Customers to edit this parameter - `<add key=" LocalFqdn"value="FQDN OF Session Remote Start SERVER"/>`
SiteId	Optional	For CVAD, fill with site ID. For Citrix DaaS, empty.
CustomerId	Optional	For CVAD, '**CitrixOnPremises**'. For Citrix DaaS, customer ID.
IcaClientName	Required	A unique hostname used for Session Remote Start initiated launches. **Must** be consistent with the value of '**$HostName**' in Logon Script DisconnectSession.ps1. Customers can leave the default "**srs-server**" parameter here. Also, keep the same in **DisconnectSession.ps1**

Parameter	Optional/Required	Description
		`<add key=" IcaClientName"value=" srs-server"/>`
MaxRequestConcurrency	Optional	The number of concurrent API requests. 100 by default.
SessionIdCacheTtlSeconds	Optional	TTL of authentication session between Session Remote Start and StoreFront. 300 by default.
DeliveryGroupsCacheTtlMinutes	Optional	TTL of Delivery Group - Tag mapping cache. 10 by default.
DesktopsCacheTtlMinutes	Optional	TTL of Desktop name cache. 10 by default.
LogToConsole	Optional	Enable console logging. Default “**False**”.
LogToConsoleLevel	Optional	Trace severity level. See Log file configuration for details. 5 by default.
LogToDebug	Optional	Developer use only.
LogToDebugLevel	Optional	Developer use only.
OverwriteLogFile	Optional	Overwrite the log file on the next service start. **False** by default.
LogFileName	Optional	Log file location. `"%AppData%\Citrix\SessionRemoteStart\Logs\SessionRemoteStart.log"` by default. If empty, no logging will occur.
LogToFileLevel	Optional	Trace severity level. See Log file configuration for details. 5 by default.

Parameter	Optional/Required	Description
LogToEventViewer	Optional	Enable event viewerlogging. Default “False”. The log path is `%SystemRoot%\System32\Winevt\Logs\Application.evtx ( Windows Logs > Application)and event source name is “ SessionRemoteStart”`.
LogToEventViewerLevel	Optional	Trace severity level. See Log file configuration for details. 5 by default.
RequestTimeoutSeconds	Optional	The timeout seconds of HTTP request from a 3rd-party service. **300** by default.
AutoRefreshConnections	Optional	**True** if Session Remote Start will auto refresh connections periodically.
UseLegacyStoreFront	Optional	**True** if StoreFront is an earlier version. **False** by default.
ProductVersion	Optional	The version of the current product build. It can be updated automatically when upgrading.
TelemetryDataDirectory	Optional	The directory of telemetry data. `"%AppData%\Citrix\SessionRemoteStart\TelemetryData"` by default even if it is empty.

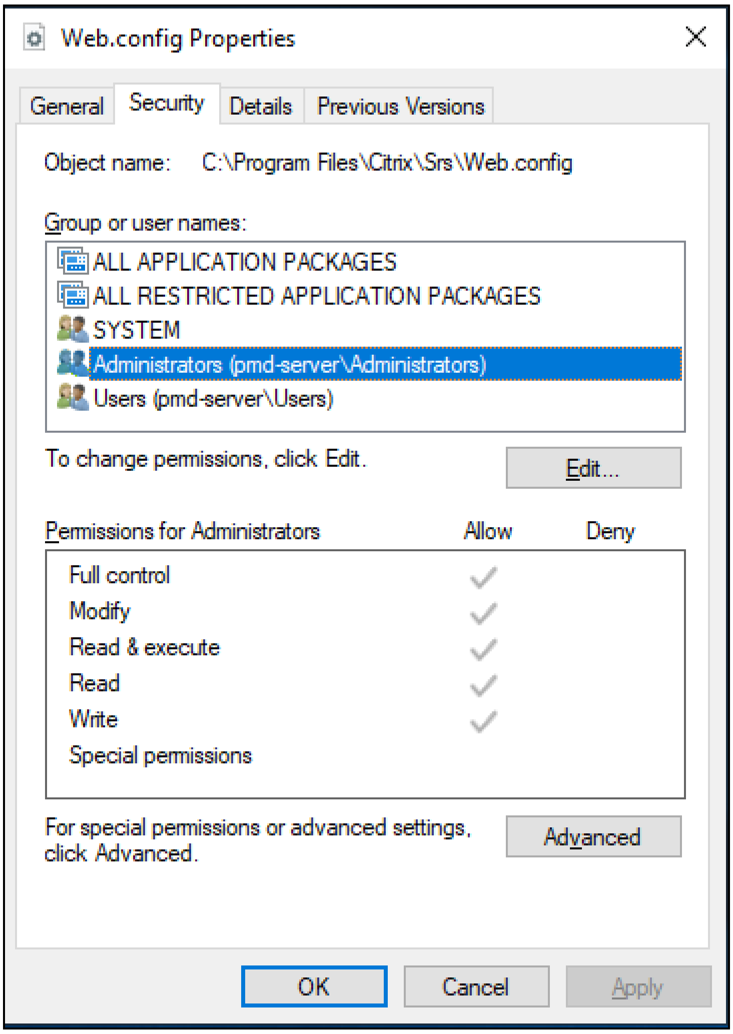
Parameter	Optional/Required	Description
LaunchDebugMode	Optional	Enable launch debug mode. Default **False**. If set to **True**, the ICA file is saved to disk instead of being launched. **Note:** For security reasons, the ICA file does not contain sensitive information. As a result, it can only be used for connection testing and cannot be used to actually launch a session.
IcaFileDirectory	Optional	The directory of ICA files. `"%AppData%\Citrix\SessionRemoteStart\IcaFiles"` by default.
IcaLog	Optional	**True** if you save the ICA communication log. **False** by default. Recommend False for saving space.
IcaLogFile	Optional	ICA log path. `"%AppData%\Citrix\SessionRemoteStart\IcaLogs"` by default.
mTLSEnabled	Optional	**True** to enable mTLS support. **False** by default.
SmartAccessFarmName	Optional	Farm name, for example: `_XD_192.168.1.19_443`
SmartAccessConditions	Optional	List of conditions, for example: `PL_WB_10.107.197.243, PL_WB_10.107.197.244`

For log-related configuration, please refer to the Log file Configuration section.

Configuration file permissions

Check permissions of Web.config: (`C:\Program Files\Citrix\SessionRemoteStart\Web.config by default`)

Make sure administrator accounts have full control while other groups/users don't have modify permission:



Object name: C:\Program Files\Citrix\Srs\Web.config

Group or user names:

- ALL APPLICATION PACKAGES
- ALL RESTRICTED APPLICATION PACKAGES
- SYSTEM
- Administrators (pmd-server\Administrators)
- Users (pmd-server\Users)

To change permissions, click Edit.

Permissions for Administrators	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
Read	✓	
Write	✓	
Special permissions		

For special permissions or advanced settings, click Advanced.

Log file Configuration

Currently, Session Remote Start logging supports CDF, AOT, and File tracing. CDF and AOT are always available. Others are based on configuration file settings.

Trace severity level

- 0 - Critical
- 1 - Urgent
- 2 - Significant
- 3 - Important
- 4 - ImportantDetailed
- 5 - Informational

- 6 - InformationalDetailed
- 7 - Notable
- 8 - NotableDetailed
- 9 - Insignificant

Log to File

Logging to file is enabled by default. To disable, set **LogFileName** in **Web.config** to empty.

The default log path is shown below, where **{Session Remote Start user}** should be replaced with the user hosting the SRS service. If the Application Pool identity has not been modified, it defaults to **SrsAppPool**. If the identity has been changed to srs, replace **{Session Remote Start user}** with **srs**.

`"C:\Users\\{ Session Remote Start user } \AppData\Roaming\Citrix\SessionRemoteStart\Logs\SessionRemoteStart.log"`.

Customers can change the log file location and permissions as per their requirements, please see the steps required to change the Log file location and permissions.

Configure Citrix Virtual Apps and Desktops REST API Credentials

January 15, 2025

This configuration is required to launch resources identified by "tags"or by "AD groups"when using the scheduling service.

Overview

During the batch pre-launch process, if the tags or AD groups are specified, Session Remote Start uses the Citrix Virtual Apps and Desktops REST API to query resources associated with those tags.

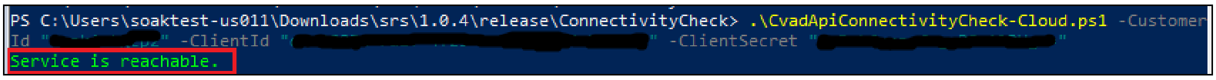
This section focuses on the steps required to configure Session Remote Start to use the Citrix Virtual Apps and Desktops REST API. It can be skipped if there are no tag-related requirements.

Confirm that Session Remote Start server can connect to Citrix Virtual Apps and Desktops REST API Service

First, check whether Session Remote Start can reach the Citrix Virtual Apps and Desktops REST API Service. Normally, this service is hosted on the DDC.

Run the test script in the package:

- For Citrix Virtual Apps and Desktops, run the `'CvadApiConnectivityCheck-OnPrem.ps1'`
- For Citrix DaaS, run the `'CvadApiConnectivityCheck-Cloud.ps1'`.



```
PS C:\Users\soaktest-us011\Downloads\srs\1.0.4\release\ConnectivityCheck> .\CvadApiConnectivityCheck-Cloud.ps1 -Customer
Id "[redacted]" -ClientId "[redacted]" -ClientSecret "[redacted]"
Service is reachable.
```

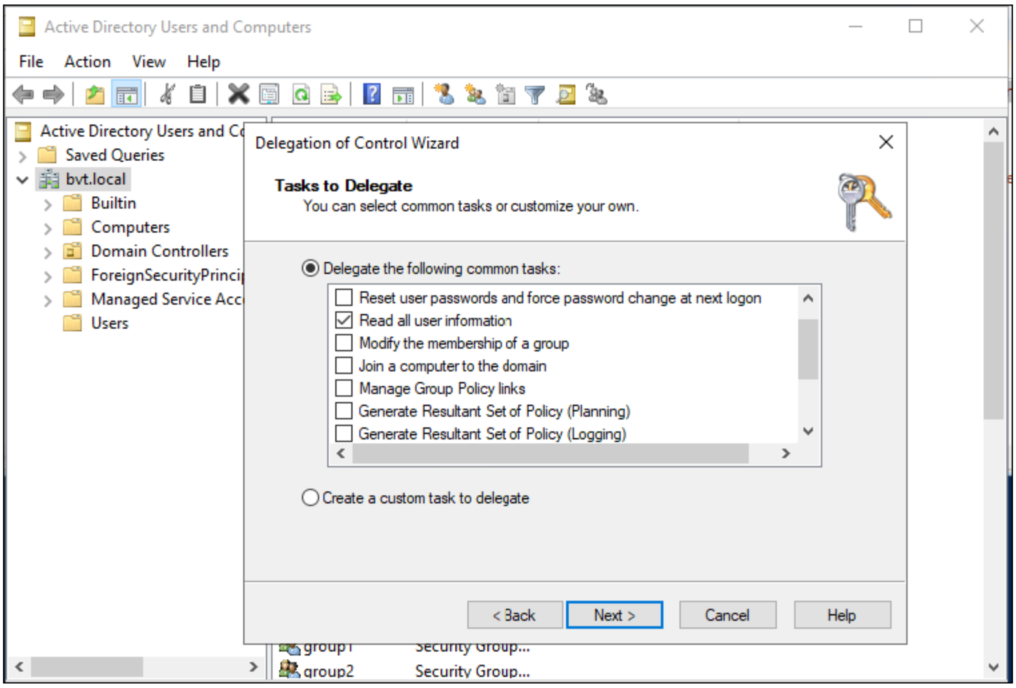
Create a user and store the Citrix Virtual Apps and Desktops REST API credentials

Session Remote Start requires a Citrix Virtual Apps and Desktops API credential to issue API requests to the REST API Service. The credential is stored under a user in the **Windows Credential Manager**.

For security reasons, avoid using a domain user if batch launch by AD group is not needed. Instead, create a local user.

Domain user On the Domain Controller, create or use an existing Domain Service Account with the **Read all user information** permission delegated.

1. Open the **Active Directory Users and Computer**.
2. In the left pane, expand the directory tree and right-click your domain.
3. Select **Delegate Control…** from the context menu to open the **Delegation of Control Wizard**.



Delegation of Control Wizard

Tasks to Delegate

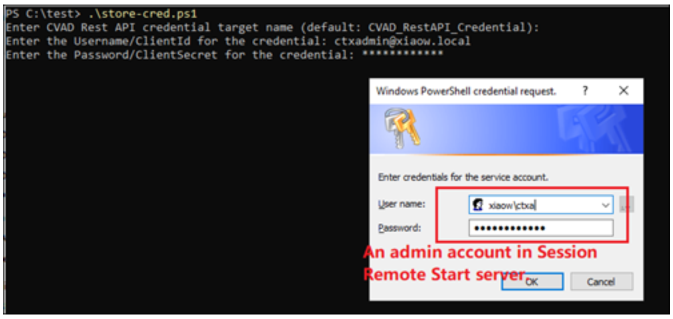
You can select common tasks or customize your own.

● Delegate the following common tasks:

- □ Reset user passwords and force password change at next logon
- ☑ Read all user information
- □ Modify the membership of a group
- □ Join a computer to the domain
- □ Manage Group Policy links
- □ Generate Resultant Set of Policy (Planning)
- □ Generate Resultant Set of Policy (Logging)

○ Create a custom task to delegate

4. On the Session Remote Start server, navigate to the **SessionRemoteStart** folder in the installation package. Run the PowerShell script `store-cred.ps1` as an administrator to configure the CVAD REST API credentials.



```
PS C:\test> .\store-cred.ps1
Enter CVAD Rest API credential target name (default: CVAD_RestAPI_Credential):
Enter the Username/ClientId for the credential: ctxadmin@xiaow.local
Enter the Password/ClientSecret for the credential: ************
```

Windows PowerShell credential request.

Enter credentials for the service account.

User name: xiaow\ctxa

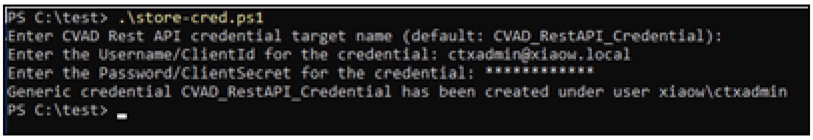
Password: ••••••••••••

An admin account in Session Remote Start server

5. For the On-prem environment, provide the admin credential. For more information, see Citrix Virtual Apps and Desktops REST APIs.

6. For the DaaS environment, provide the client identity. For more information, see Citrix Cloud APIs.

A success message is displayed upon completion.



```
PS C:\test> .\store-cred.ps1
Enter CVAD Rest API credential target name (default: CVAD_RestAPI_Credential):
Enter the Username/ClientId for the credential: ctxadmin@xiaow.local
Enter the Password/ClientSecret for the credential: ************
Generic credential CVAD_RestAPI_Credential has been created under user xiaow\ctxadmin
PS C:\test> _
```

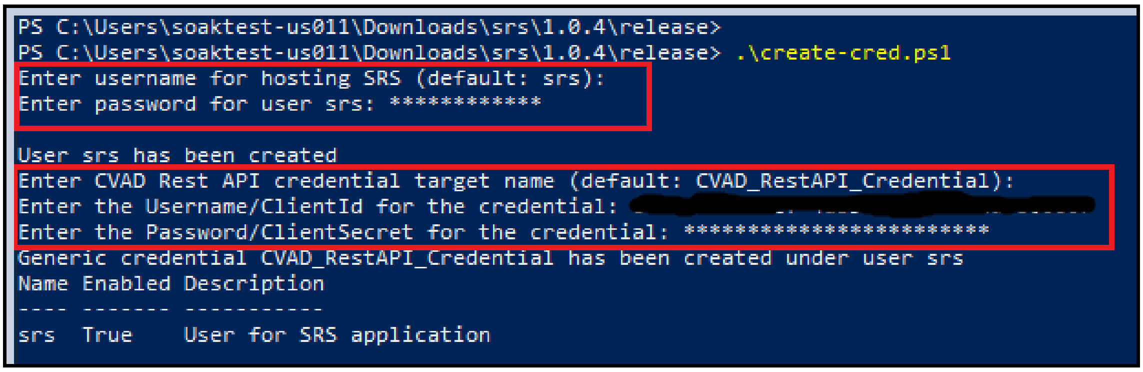
Local user The `create-cred.ps1` script handles both tasks, creating the local user and storing the credential.

From the installation package, under the **SessionRemoteStart** folder, run the script **create-cred.ps1** as an administrator. This will:

1. Create a local user for hosting Session Remote Start.

2. Configure the Citrix Virtual Apps and Desktops REST API credentials.

    - For Citrix Virtual Apps and Desktops environment, provide the admin credential. (More details are here)
    - For the Citrix DaaS environment, provide the client identity. (More details are here)



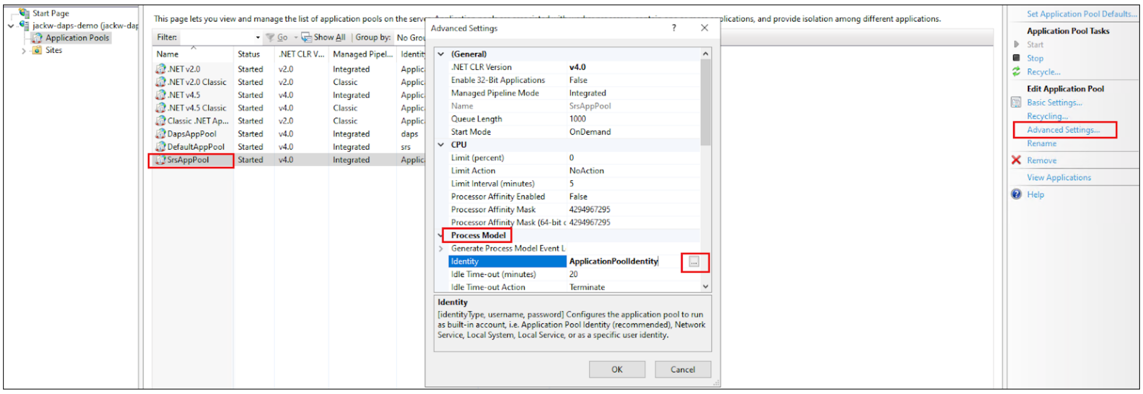
```
PS C:\Users\soaktest-us011\Downloads\srs\1.0.4\release>
PS C:\Users\soaktest-us011\Downloads\srs\1.0.4\release> .\create-cred.ps1
Enter username for hosting SRS (default: srs):
Enter password for user srs: ************

User srs has been created
Enter CVAD Rest API credential target name (default: CVAD_RestAPI_Credential):
Enter the Username/ClientId for the credential: [redacted]
Enter the Password/ClientSecret for the credential: ************************
Generic credential CVAD_RestAPI_Credential has been created under user srs
Name Enabled Description
---- ------- -----------
srs  True    User for SRS application
```

Configure Session Remote Start Application Pool

Overview

By default, IIS runs an application (site or service) under the **ApplicationPoolIdentity** for each unique application pool. Configure Session Remote Start to run under the previously created user identity by setting the Session Remote Start application pool to use the custom user:

1. Highlight `SrsAppPool` from the Application Pools and select **Advanced Settings** under the **Edit Application Pool**. Scroll down to **Process Model > Identity** and click the three dots.



Name	Status	.NET CLR V...	Managed Pipel...	Identit
.NET v2.0	Started	v2.0	Integrated	Applic
.NET v2.0 Classic	Started	v2.0	Classic	Applic
.NET v4.5	Started	v4.0	Integrated	Applic
.NET v4.5 Classic	Started	v4.0	Classic	Applic
Classic .NET Ap...	Started	v2.0	Classic	Applic
DapsAppPool	Started	v4.0	Integrated	daps
DefaultAppPool	Started	v4.0	Integrated	srs
SrsAppPool	Started	v4.0	Integrated	Applic

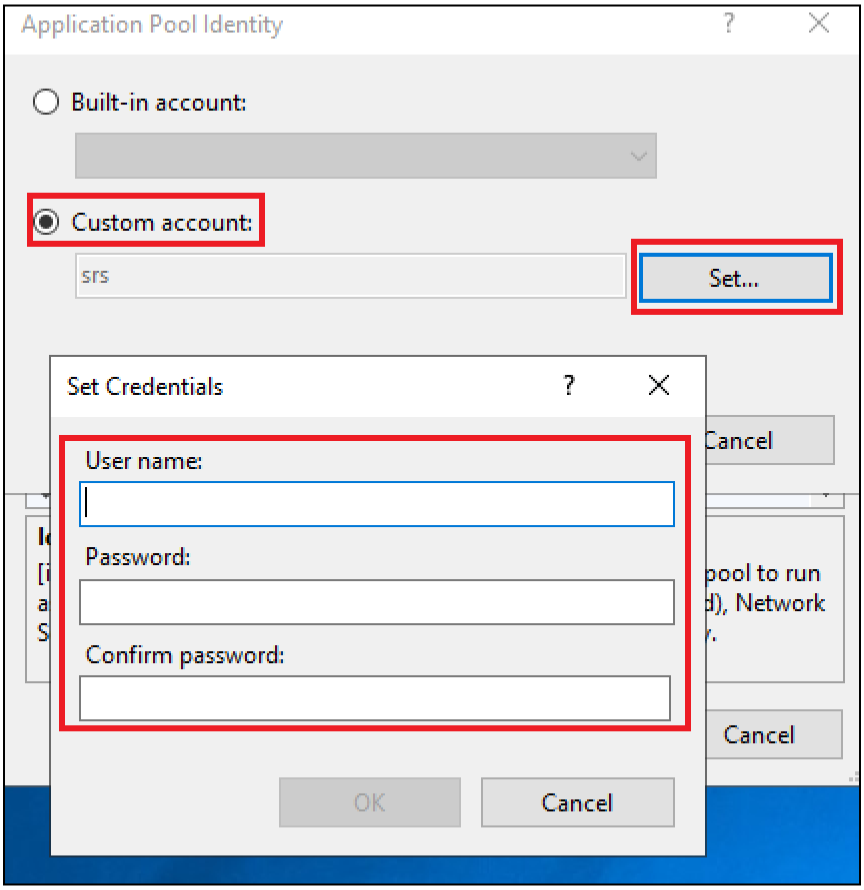
Advanced Settings

(General)	
.NET CLR Version	**v4.0**
Enable 32-Bit Applications	False
Managed Pipeline Mode	Integrated
Name	SrsAppPool
Queue Length	1000
Start Mode	OnDemand
CPU	
Limit (percent)	0
Limit Action	NoAction
Limit Interval (minutes)	5
Processor Affinity Enabled	False
Processor Affinity Mask	4294967295
Processor Affinity Mask (64-bit c	4294967295
Process Model	
Generate Process Model Event L	
Identity	**ApplicationPoolIdentity**
Idle Time-out (minutes)	20
Idle Time-out Action	Terminate

Identity
[identityType, username, password] Configures the application pool to run as built-in account, i.e. Application Pool Identity (recommended), Network Service, Local System, Local Service, or as a specific user identity.

OK Cancel

Select **Custom account**, click **Set**, and enter the **username** and **password** of the user created for hosting Session Remote Start.



> **Note:**
>
> To manage AD groups instead of the user list, use the Domain Service Account configured in Create a user and store the CVAD REST API credentials.

2. Ensure the Application Pool's **setProfileEnvironment** attribute is enabled.

   - Navigate to the `%windir%/system32/inetsrv/config` folder.
   - Open the `applicationHost.config` file.
   - Locate the `<system.applicationHost><applicationPools><SrsAppPool><processModel>` element.
   - Confirm that the `setProfileEnvironment` attribute is not present, which defaults the value to true, or explicitly sets the attribute's value to true.

> **Note:**
>
> Ensure to restart `SessionRemoteStart` in IIS Manager UI or run `iisreset` command from the command prompt.

Configure Inbound Firewall Rules: Customers can specify the IP addresses and host names of the trusted services and StoreFront ensures that only these sources can communicate with Session Remote Start, see Configure Inbound Firewall Rules for steps.

StoreFront Configuration

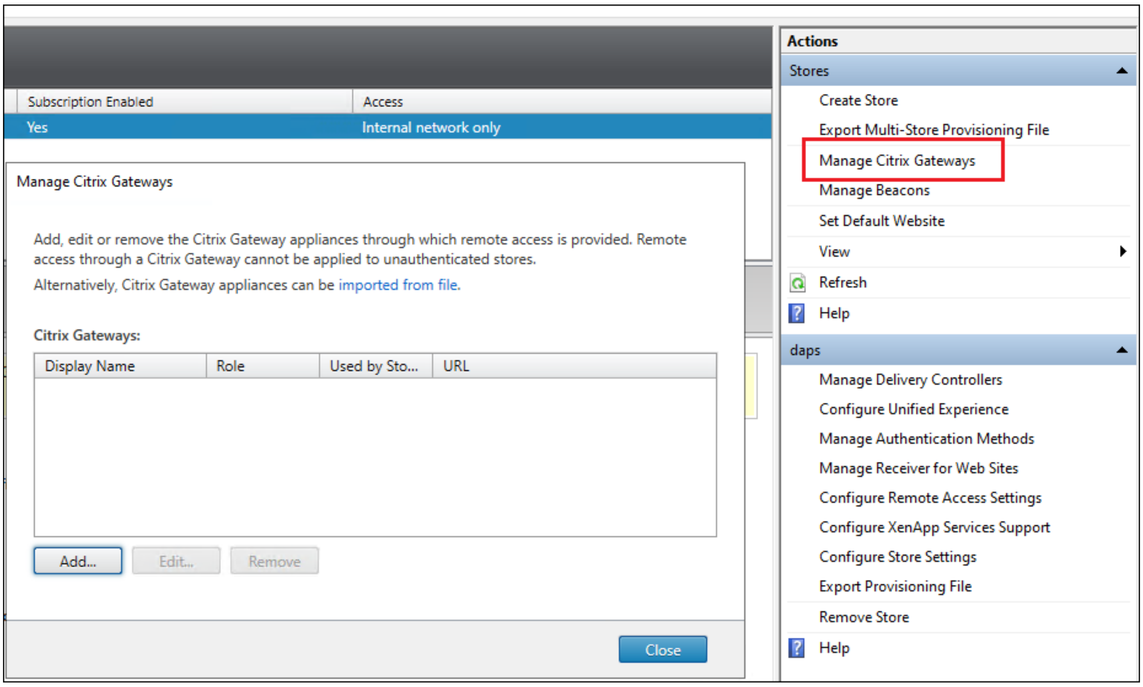
December 11, 2024

Install SSL certificate for accessing Session Remote Start

For ease of deployment, each Session Remote Start server is configured as a special type of Gateway with StoreFront. As such, StoreFront must be able to contact Session Remote Start at the specified Gateway callback URL (`https://<Session Remote Start FQDN>/SessionRemoteStart/CitrixAuthService/AuthService.asmx`).

Add Session Remote Start as a Gateway

1. Click **Manage Citrix Gateways** in the **Stores** panel on the right.



Subscription Enabled	Access
Yes	Internal network only

Manage Citrix Gateways

Add, edit or remove the Citrix Gateway appliances through which remote access is provided. Remote access through a Citrix Gateway cannot be applied to unauthenticated stores.

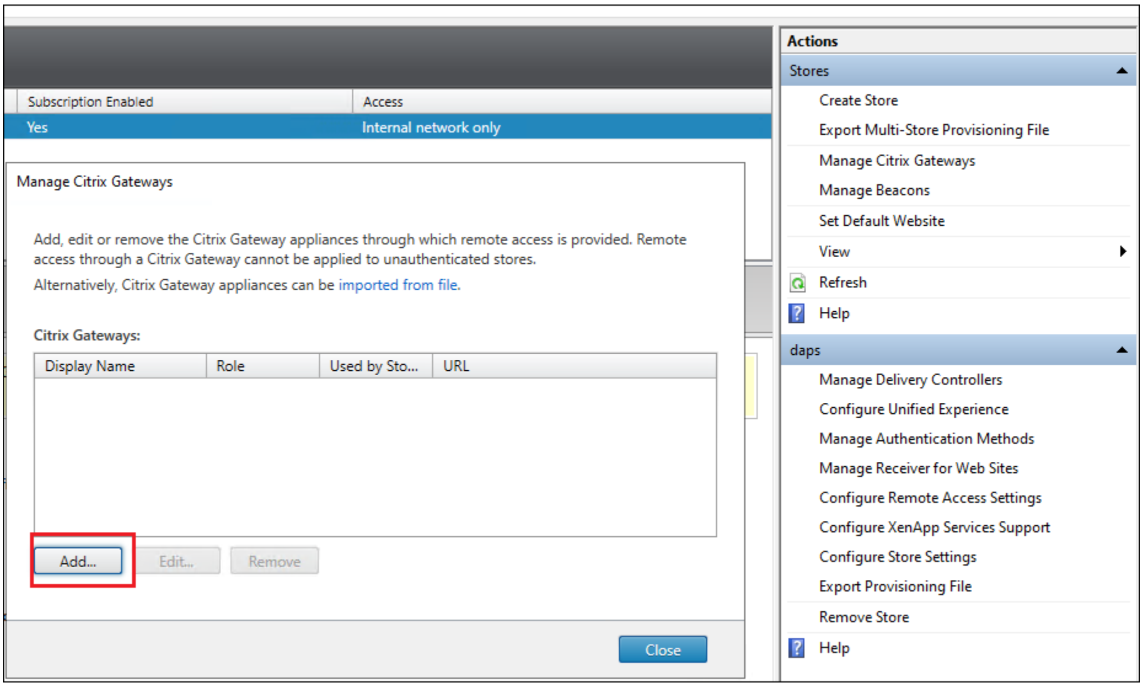
Alternatively, Citrix Gateway appliances can be imported from file.

Citrix Gateways:

Display Name	Role	Used by Sto...	URL

Add...
Edit...
Remove
Close
Actions
Stores
Create Store
Export Multi-Store Provisioning File
Manage Citrix Gateways
Manage Beacons
Set Default Website
View
Refresh
Help
daps
Manage Delivery Controllers
Configure Unified Experience
Manage Authentication Methods
Manage Receiver for Web Sites
Configure Remote Access Settings
Configure XenApp Services Support
Configure Store Settings
Export Provisioning File
Remove Store
Help

2. Add a new gateway.



Subscription Enabled	Access
Yes	Internal network only

Manage Citrix Gateways

Add, edit or remove the Citrix Gateway appliances through which remote access is provided. Remote access through a Citrix Gateway cannot be applied to unauthenticated stores.

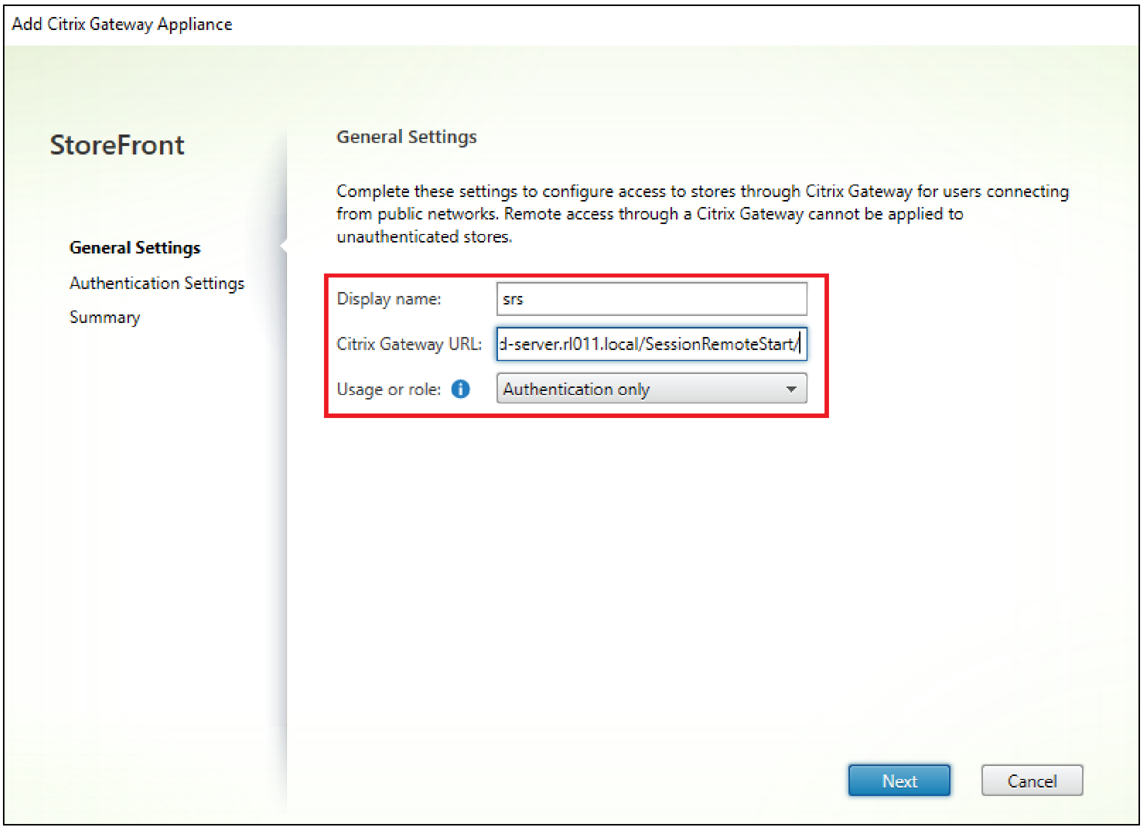
Alternatively, Citrix Gateway appliances can be imported from file.

Citrix Gateways:

Display Name	Role	Used by Sto...	URL

Add...
Edit...
Remove
Close
Actions
Stores
Create Store
Export Multi-Store Provisioning File
Manage Citrix Gateways
Manage Beacons
Set Default Website
View
Refresh
Help
daps
Manage Delivery Controllers
Configure Unified Experience
Manage Authentication Methods
Manage Receiver for Web Sites
Configure Remote Access Settings
Configure XenApp Services Support
Configure Store Settings
Export Provisioning File
Remove Store
Help

3. Set Display name, set Citrix Gateway URL with `https://<Session Remote Start FQDN>/SessionRemoteStart/`, and change **Usage or role** to **Authentication only**.



Add Citrix Gateway Appliance

General Settings

Complete these settings to configure access to stores through Citrix Gateway for users connecting from public networks. Remote access through a Citrix Gateway cannot be applied to unauthenticated stores.

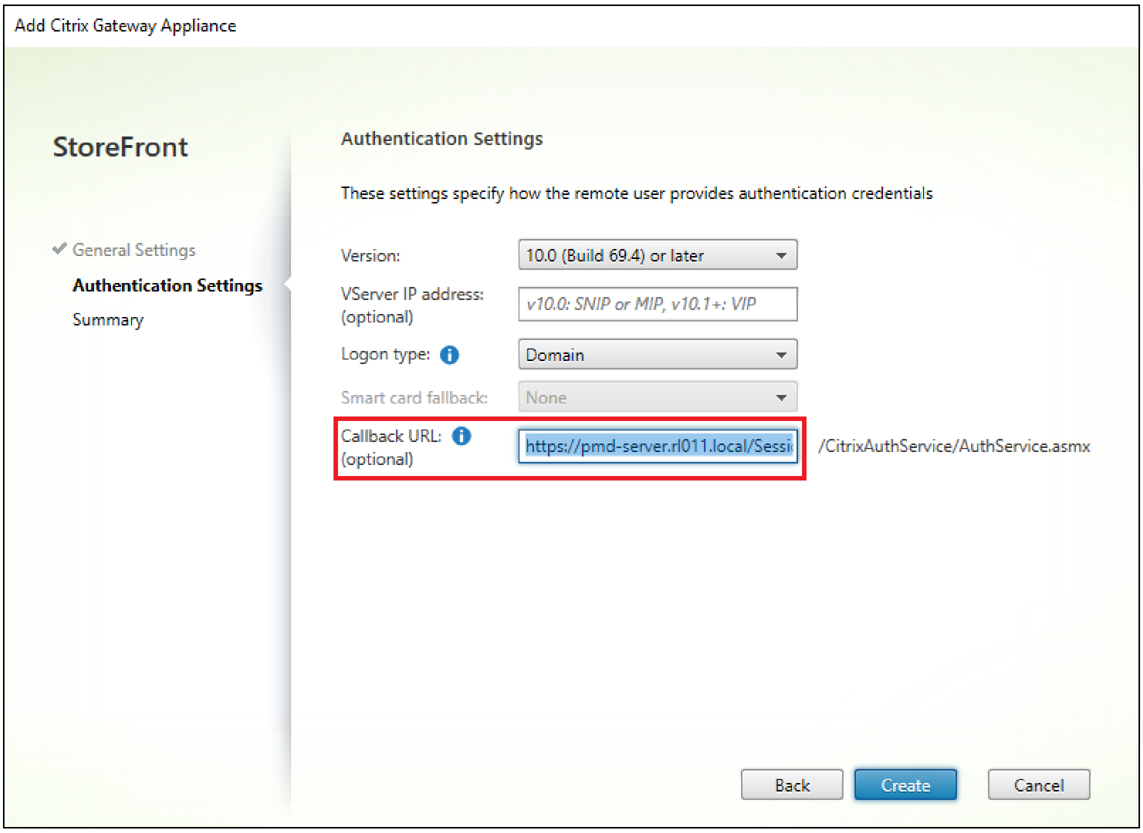
Display name: srs

Citrix Gateway URL: d-server.rl011.local/SessionRemoteStart/

Usage or role: Authentication only

4. Set Callback URL with `https://<Session Remote Start FQDN>/SessionRemoteStart`

.



Add Citrix Gateway Appliance

StoreFront

✓ General Settings

Authentication Settings

Summary

Authentication Settings

These settings specify how the remote user provides authentication credentials

Version: 10.0 (Build 69.4) or later

VServer IP address: (optional) v10.0: SNIP or MIP, v10.1+: VIP

Logon type: Domain

Smart card fallback: None

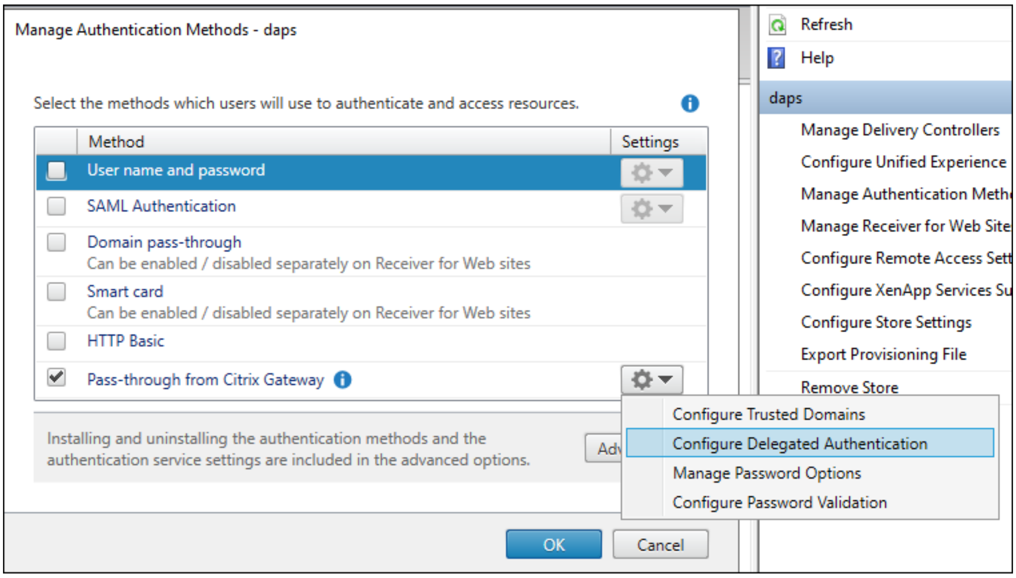
Callback URL: (optional) https://pmd-server.rl011.local/Sessi /CitrixAuthService/AuthService.asmx

Create a New Store for Session Remote Start

Although an existing Store can be used, it is recommended that a new Store should be created specifically for Session Remote Start usage.

Manage Authentication Methods

1. On the new Store, find the **Manage Authentication Methods** in the Store configuration panel on the right.
2. Ensure the **Pass-through from Citrix Gateway** is checked.
3. Expand settings, Click **Configure Delegated Authentication**.



Manage Authentication Methods - daps

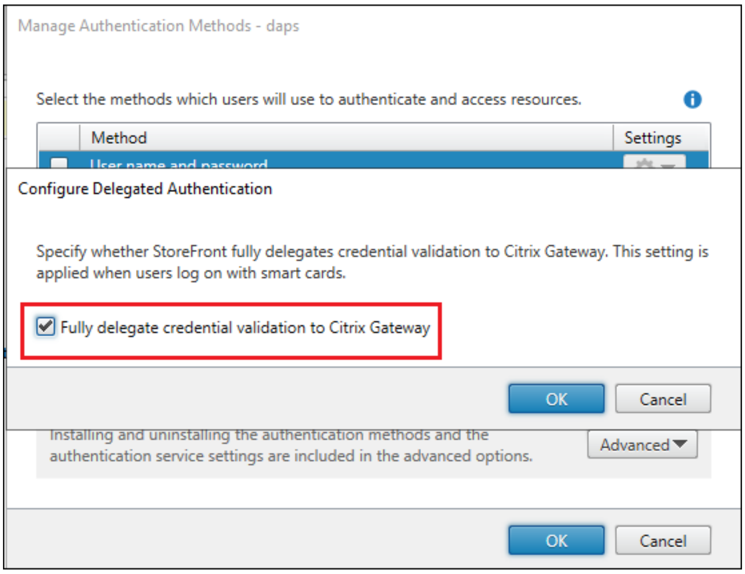
Select the methods which users will use to authenticate and access resources.

	Method	Settings
□	User name and password	
□	SAML Authentication	
□	Domain pass-through Can be enabled / disabled separately on Receiver for Web sites	
□	Smart card Can be enabled / disabled separately on Receiver for Web sites	
□	HTTP Basic	
☑	Pass-through from Citrix Gateway	

Installing and uninstalling the authentication methods and the authentication service settings are included in the advanced options.

Adv
OK
Cancel
Refresh
Help
daps
Manage Delivery Controllers
Configure Unified Experience
Manage Authentication Meth
Manage Receiver for Web Site
Configure Remote Access Sett
Configure XenApp Services Su
Configure Store Settings
Export Provisioning File
Remove Store
Configure Trusted Domains
Configure Delegated Authentication
Manage Password Options
Configure Password Validation

4. Enable the **Full delegate credential validation to Citrix Gateway**.



Manage Authentication Methods - daps

Select the methods which users will use to authenticate and access resources.

Configure Delegated Authentication

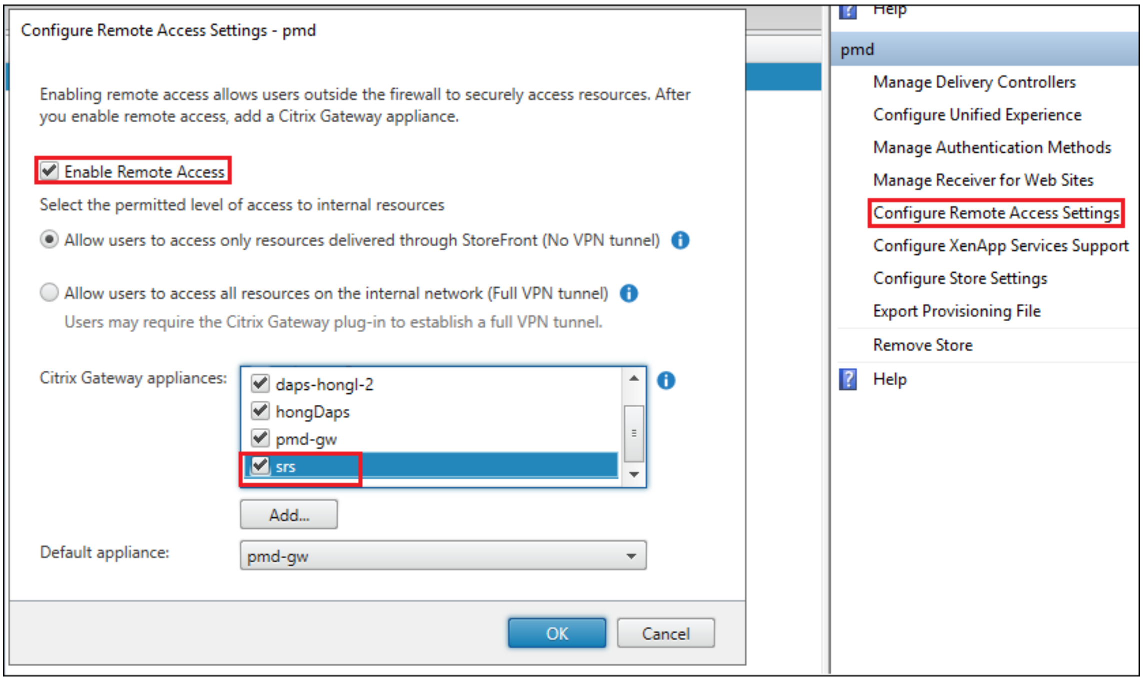
Specify whether StoreFront fully delegates credential validation to Citrix Gateway. This setting is applied when users log on with smart cards.

☑ Fully delegate credential validation to Citrix Gateway

Installing and uninstalling the authentication methods and the authentication service settings are included in the advanced options.

Configure Remote Access Settings

1. Click **Configure Remote Access Settings** in the Store configuration panel on the right.
2. Enable the **Remote Access**.
3. Select the Gateway configured above.



Configure Remote Access Settings - pmd

Enabling remote access allows users outside the firewall to securely access resources. After you enable remote access, add a Citrix Gateway appliance.

☑ Enable Remote Access

Select the permitted level of access to internal resources

● Allow users to access only resources delivered through StoreFront (No VPN tunnel)

○ Allow users to access all resources on the internal network (Full VPN tunnel)

Users may require the Citrix Gateway plug-in to establish a full VPN tunnel.

Citrix Gateway appliances: ☑ daps-hongl-2 ☑ hongDaps ☑ pmd-gw ☑ srs

Default appliance: pmd-gw

Add...
OK
Cancel
Help
pmd
Manage Delivery Controllers
Configure Unified Experience
Manage Authentication Methods
Manage Receiver for Web Sites
Configure Remote Access Settings
Configure XenApp Services Support
Configure Store Settings
Export Provisioning File
Remove Store
Help

Configure Session Remote Start plugin

This plugin should be applied to the store that the end user is using, not the Session Remote Start store.

1. Backup Existing plugins:
   On the StoreFront server, go to the following website dir, `'C:\inetpub\wwwroot\Citrix\%StoreName%\'`, open `'bin'` folder.
   Backup the existing **StoreCustomization_Input.dll**, **StoreCustomization_Enumeration.dll** to a specific directory. e.g. `'C:\stf_original_plugin'`.
2. Paste the Citrix team provided three DLLs to the bin folder - **StoreCustomization_Input.dll**, **StoreCustomization_Enumeration.dll**, **SrsStoreFrontPluginCommon.dll**.
3. Set up system environment:

   - Open System (Control Panel).
   - Click the Advanced system settings link.
   - Click **Environment Variables**.
   - Add **New…** in the System variables section, In the **New System Variable** window, add below environment variables. Click **OK**. Close all remaining windows by clicking **OK**.

Variable Name	Required/Optional	Description	Example
`srs_server_urls`	Required	Session Remote Start server URL	`https://pmd-server.rl011.local/SessionRemoteStart`
`stf_original_plugins_path`	Optional	Original plugins directory	`C:\stf_original_plugin`
`launching_suffix`	Optional	Resource title suffix while preparing by Session Remote Start. If not configured, ‘-Preparing’by default.	- Preparing

4. Grant access to `stf_original_plugins_path`. Similar to Session Remote Start file permission configuration, grant access to StoreFront application pool identity.
5. Restart IIS service - `iisreset`.

Configure DDC

December 12, 2024

Enable TrustRequestsSentToTheXmlServicePort

Required by the DDC to allow Session Remote Start requests via Storefront to be trusted.

For Citrix Virtual Apps and Desktops

Run the following commandlets on the Delivery Controller:

```
asnp Citrix*
Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true
```

For Citrix DaaS

Run the following commandlets:

1. On a machine with internet connection, install Citrix DaaS Remote PowerShell SDK
   Other articles also contain related information:
2. Open PowerShell, run the following
   ```
   Get-XdAuthentication
   ```
   An authentication dialog opens.
3. Execute the commandlets as On-Prem
   ```
   asnp Citrix*
   Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true
   ```
4. Sign out.
   ```
   Clear-XDCredentials
   ```

App Protection: If customers have an App protected delivery group, see App Protection.

HTTP Proxy: If customers have configured HTTP proxies in their setup, see HTTP Proxy Configuration.

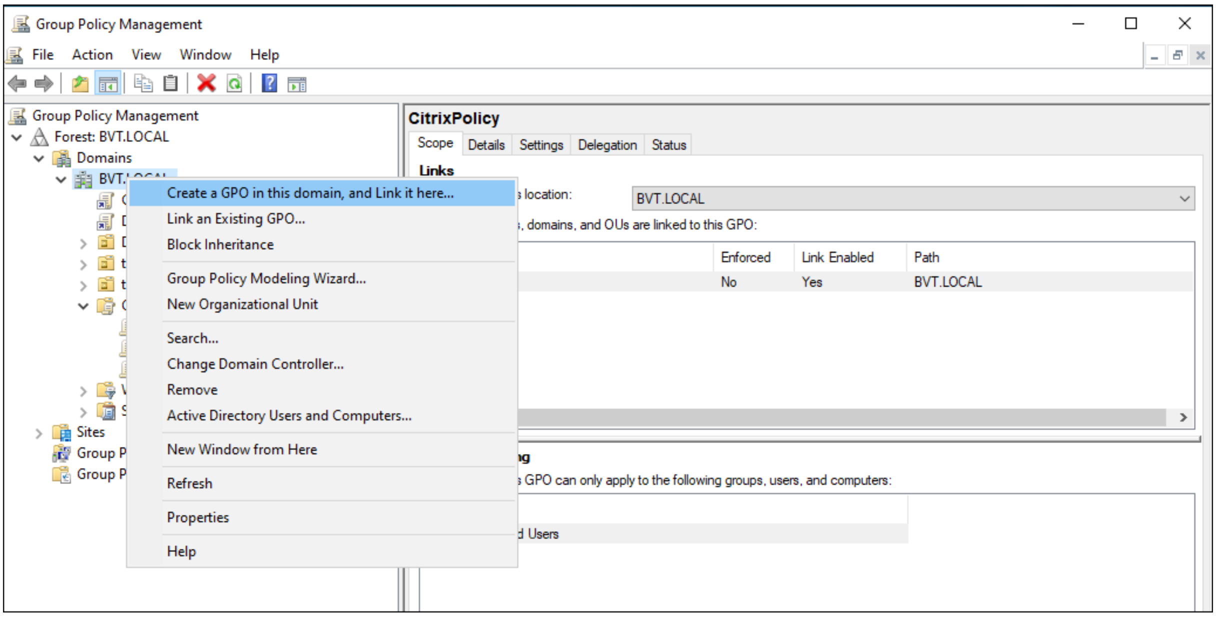
Configure Logon script for AD server

December 11, 2024

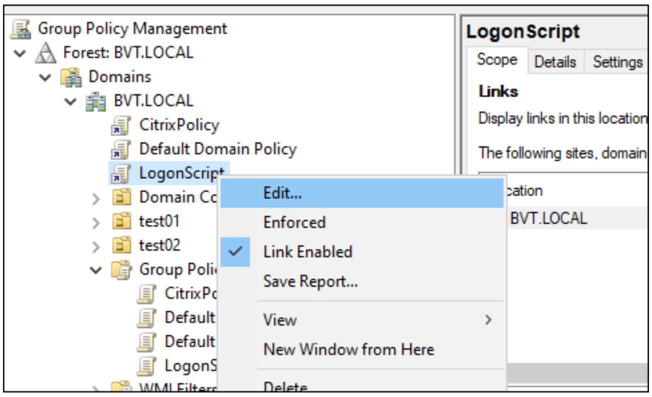
The Logon script is used by the VDA to disconnect the pre-launch session after the Session Remote Start initiated logon completes. We use Group Policy to apply the script to all VDAs and users.

Steps to create a GPO and link it to a Domain

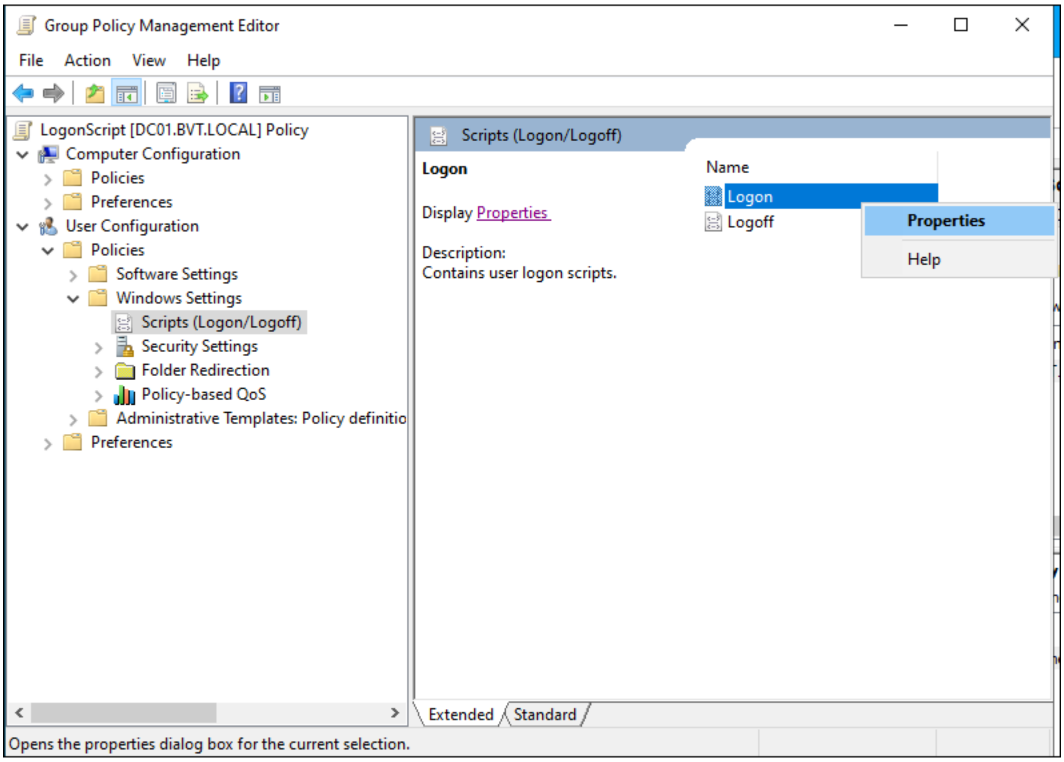
1. On the Windows domain controller, open **Group Policy Management** and create a GPO under the domain.


Group Policy Management
File Action View Window Help
Group Policy Management
Forest: BVT.LOCAL
Domains
Sites
CitrixPolicy
Scope Details Settings Delegation Status
Links
BVT.LOCAL
Enforced Link Enabled Path
No Yes BVT.LOCAL
Create a GPO in this domain, and Link it here...
Link an Existing GPO...
Block Inheritance
Group Policy Modeling Wizard...
New Organizational Unit
Search...
Change Domain Controller...
Remove
Active Directory Users and Computers...
New Window from Here
Refresh
Properties
Help

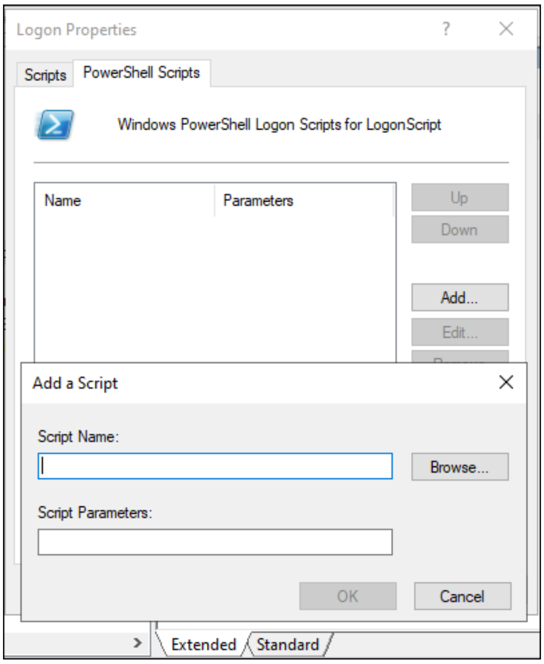
1. Right-click on the GPO, select **Edit** to open the Group Policy Management Editor.



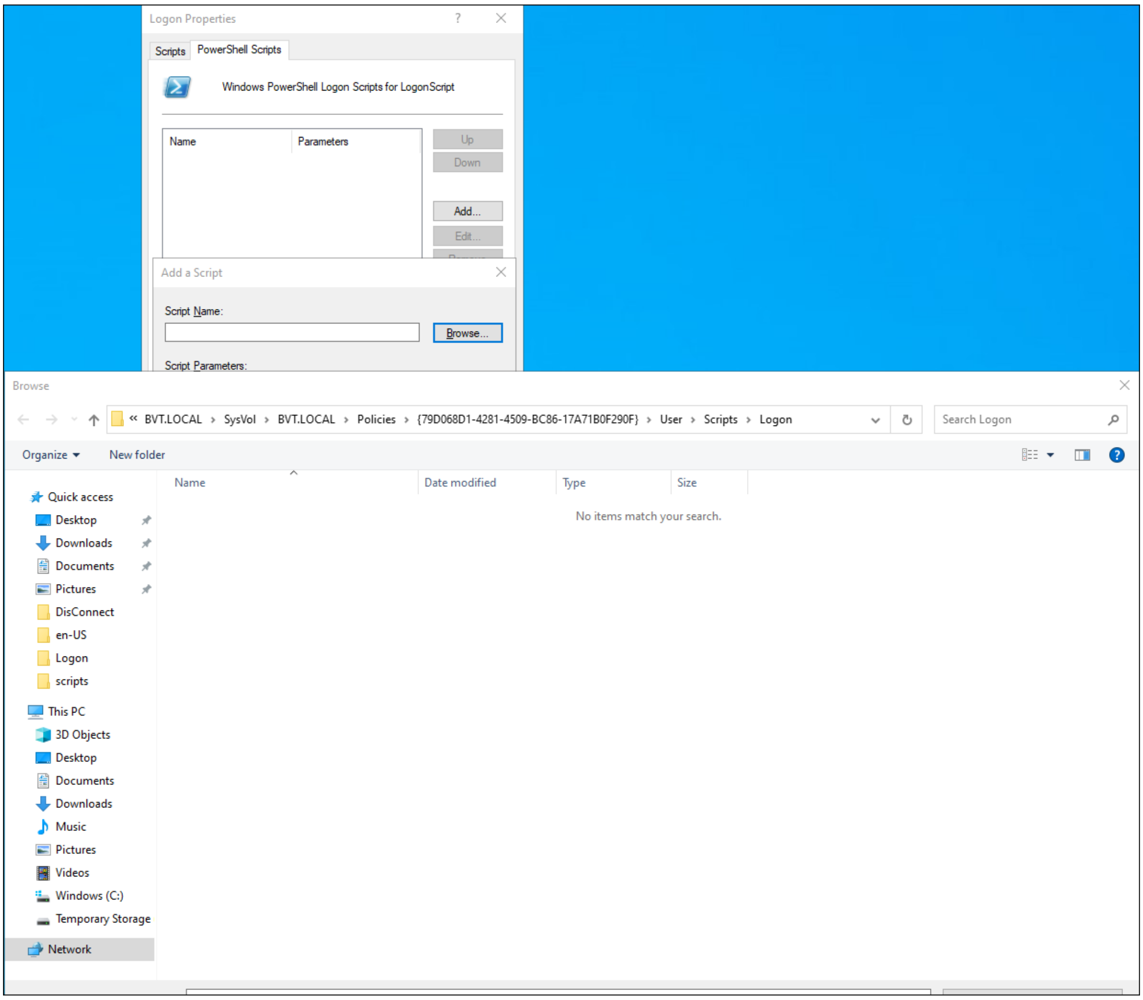
1. In the **Group Policy Management Editor**, expand **User Configuration > Policies > Windows Settings > Scripts (Logon/Logoff)**. Right-click **Logon on** in the right panel and select **Properties**.



2. Switch to the **PowerShell Scripts** tab, and click **Add…**.

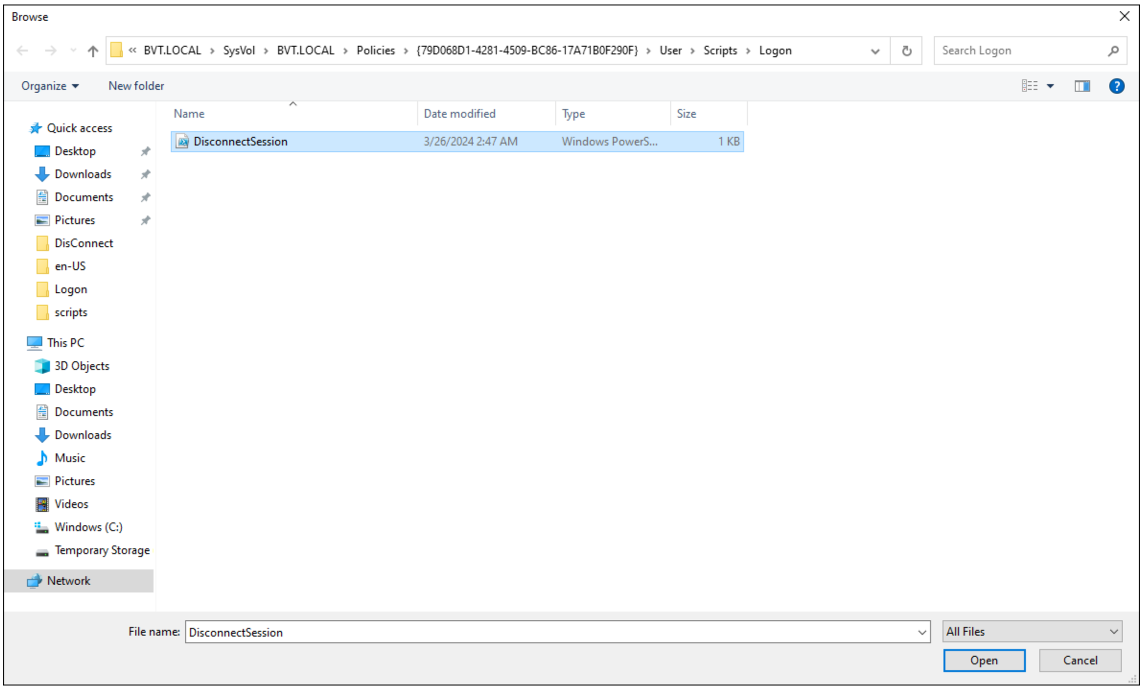


3. Click **Browse…** on the right of 'Script Name'field, a file browser pops up, located in the **NetLogon** folder by default.



The Logon folder is a shared folder which typically has read-only and execute permissions by machines and users. To avoid permission issues, it is recommended not to use any other folder.

1. Create **DisconnectSession.ps1** under this folder. (Please use the one provided by Citrix as part of the installation file).



Browse

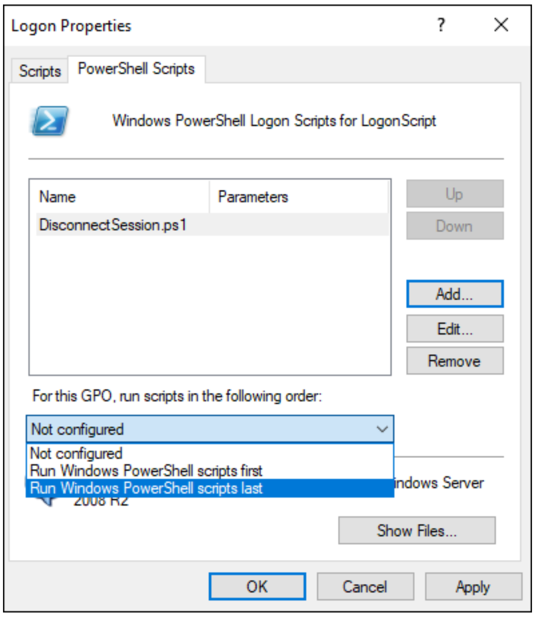
« BVT.LOCAL › SysVol › BVT.LOCAL › Policies › {79D068D1-4281-4509-BC86-17A71B0F290F} › User › Scripts › Logon

Name	Date modified	Type	Size
DisconnectSession	3/26/2024 2:47 AM	Windows PowerS…	1 KB

File name: DisconnectSession

All Files

2. Select **Run Windows PowerShell scripts last** and click **OK** or **Apply**.



Logon Properties

Scripts | PowerShell Scripts

Windows PowerShell Logon Scripts for LogonScript

Name	Parameters
DisconnectSession.ps1	

For this GPO, run scripts in the following order:

Not configured

- Not configured
- Run Windows PowerShell scripts first
- Run Windows PowerShell scripts last

Configure Citrix FAS

Steps to Install and configure FAS

To install and configure FAS in your setup, see Install and configure.

FAS Do's and Dont's

1. It is mandatory to enable the FAS plug-in on **StoreFront** stores as we are using Citrix Virtual Apps and Desktops StoreFront.
2. Check the rule on your FAS server, to ensure your STF is allowed in the **Manage StoreFront Permissions** page.

   > **Note:**
   >
   > - Be aware that by default, there is a DENY entry for Domain Computers. On windows DENY always "wins".
   > - Please check that the permissions from Storefront servers for groups such as domain computers is not set to Deny?
   > - Verify if **FAS rules > access control > domain computers** is set to **Allow**.

3. Ensure the domain users are added in the FAS console.

   a) **FAS console > Rule Default > restrictions > Manage user permissions** check if you have the domain user here.
   b) Set the Domain users for FAS user authentication in the FAS console to **allowed**.

4. Storefront servers should be authorized to use FAS by default, if not please do it explicitly.

   a) On the FAS server Open Citrix Federated Authentication Service console
   b) Go to Rules tab, select the appropriate policy and click on pencil icon edit
   c) On the left menu select **Access control**, click the **Manage StoreFront access permissions** link.
   d) In the **Permission for StoreFront Servers** page, add your StoreFront servers and give them the **Assert Identity** permission and click **OK**.

Telemetry

December 12, 2024

Telemetry data collection is mandatory while Session Remote Start administrators can change the data location. For more information, see Log file configuration. The directory of telemetry data. `"%AppData%\Citrix\SessionRemoteStart\TelemetryData"`

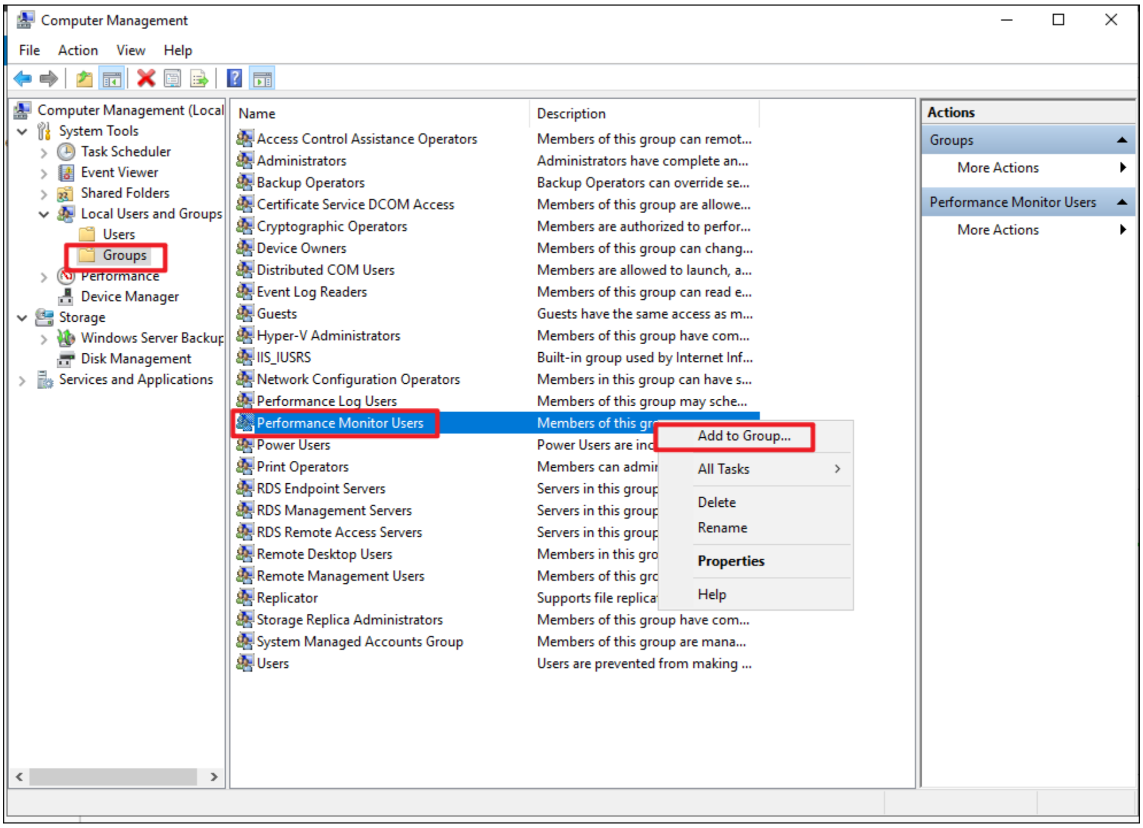
Session Remote Start server is designed to capture the following data:

- Metrics of API requests, which are saved in **RequestData.csv**.
- Metrics of server performance of CPU and memory, which are saved in **UsageData.csv**.

Grant permission for IIS Application Pool for Telemetry

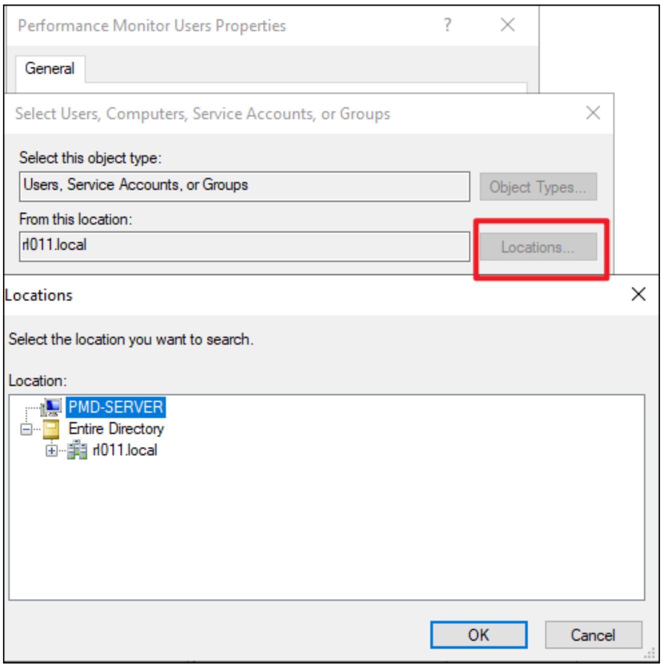
The following steps are required to make the IIS Application Pool have the permission to collect performance monitor data.

1. On the Session Remote Start server, open and select **System Tools > Local Users and Groups > Groups**. Then right-click **Performance Monitor Users** on the right panel and select **Add to Group...**.



Name	Description
Access Control Assistance Operators	Members of this group can remot...
Administrators	Administrators have complete an...
Backup Operators	Backup Operators can override se...
Certificate Service DCOM Access	Members of this group are allowe...
Cryptographic Operators	Members are authorized to perfor...
Device Owners	Members of this group can chang...
Distributed COM Users	Members are allowed to launch, a...
Event Log Readers	Members of this group can read e...
Guests	Guests have the same access as m...
Hyper-V Administrators	Members of this group have com...
IIS_IUSRS	Built-in group used by Internet Inf...
Network Configuration Operators	Members in this group can have s...
Performance Log Users	Members of this group may sche...
Performance Monitor Users	Members of this gr
Power Users	Power Users are inc
Print Operators	Members can admi
RDS Endpoint Servers	Servers in this group
RDS Management Servers	Servers in this group
RDS Remote Access Servers	Servers in this group
Remote Desktop Users	Members in this gro
Remote Management Users	Members of this grc
Replicator	Supports file replica
Storage Replica Administrators	Members of this group have com...
System Managed Accounts Group	Members of this group are mana...
Users	Users are prevented from making ...

2. Click **Add..** and then click **Locations...** and select your local computer.



Performance Monitor Users Properties

Select Users, Computers, Service Accounts, or Groups

Select this object type:

Users, Service Accounts, or Groups

From this location:

rl011.local

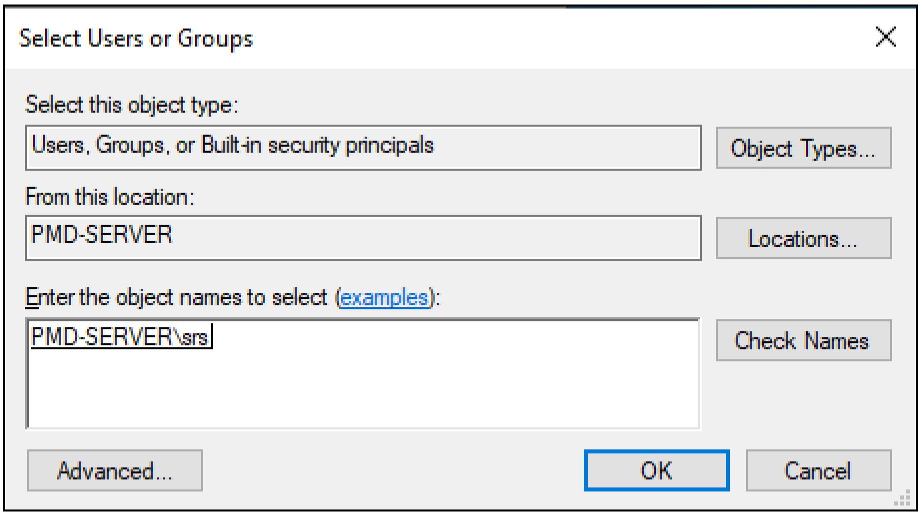
Locations

Select the location you want to search.

Location:

PMD-SERVER
Entire Directory
rl011.local

3. Input the Session Remote Start user created in the previous section. (If the default identity is used, input **IIS AppPool\SrsAppPool** instead.)



Select Users or Groups

Select this object type:

Users, Groups, or Built-in security principals

From this location:

PMD-SERVER

Enter the object names to select (examples):

PMD-SERVER\srs

4. Open PowerShell, and run the following commandlet:

```
iisreset
```

Installation checklist

December 11, 2024

Session Remote Start Server

1. Open `<https://<baseURL>/Citrix/<storename>Web>` and verify if the page opens.

> **Note:**
>
> Ignore the **No logon methods are available on this platform** message.

1. If **LogFileName** is configured, check file existence, check for any errors in the log.

3rd-party Auth Service Server

1. Open `<https://<Session Remote Start FQDN>/SessionRemoteStart/CitrixAuthService/AuthService.asmx>` and verify if it opens without a warning.

StoreFront Server

1. Open `<https://<Session Remote Start FQDN>/SessionRemoteStart/CitrixAuthService/AuthService.asmx>` and verify if it opens without warning.
2. Double check the configurations, including:

    a) Gateway, especially double check the gateway URL and callback URL must be Session Remote Start server.
    b) Authentication methods, especially **Delegated Authentication**.
    c) Remote Access, specifically applies to the gateway configured above.

3. Enable FAS plug-in on storefront stores. Federated Authentication Service integration should be enabled on a StoreFront Store using the PowerShell script.

DDC

Check if **TrustRequestsSentToTheXmlServicePort** is enabled. (How to run the following commandlets please refer to DDC Configuration)

```
asnp Citrix*
Get-BrokerSite
```

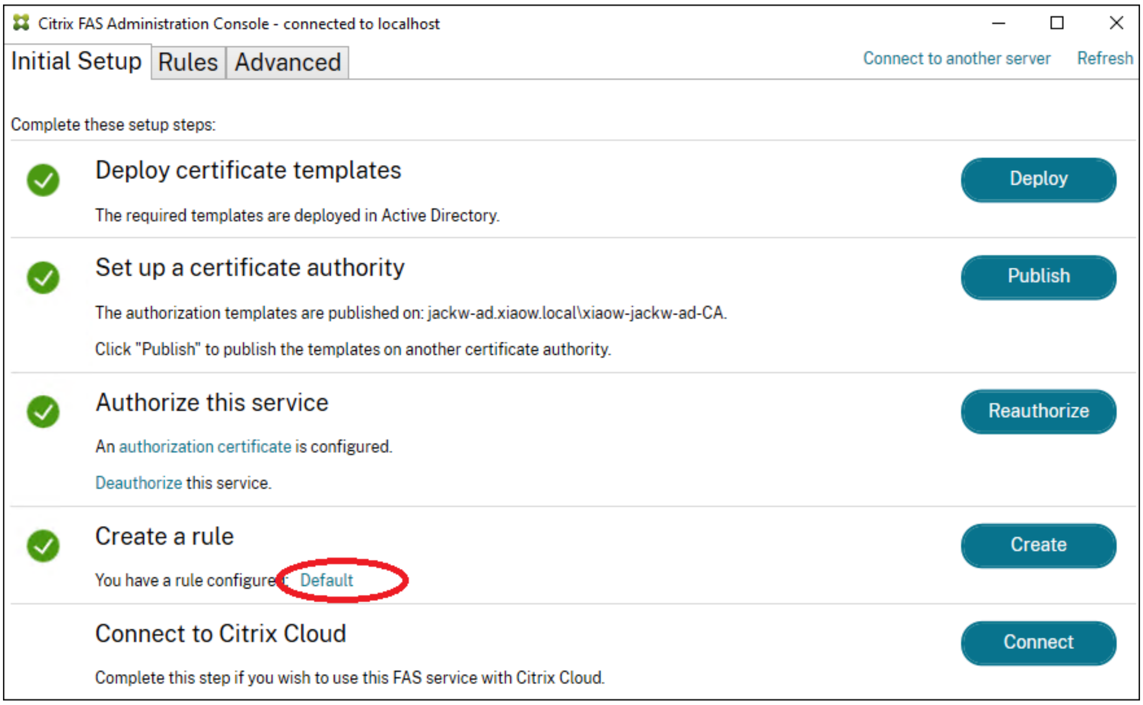
AD

Verify if the logon script is configured.

FAS

If FAS has never been installed before, and it is specifically for the installation of Session Remote Start, please ensure that FAS is correctly configured and functional.

1. Reconfirm that FAS plug-in is enabled on StoreFront, as mentioned in StoreFront checklist using the PowerShell script.
2. Reconfirm that DDC trust the StoreFront servers requests, as mentioned in DDC checklist (**TrustRequestsSentToTheXmlServicePort** enabled).
3. Confirm that Group Policy is correctly configured, especially FAS FQDN is configured. Confirm Group Policy is applied to all necessary machines (StoreFront/VDA/DDC).
4. Confirm the user rules. If the default rule is used for quick FAS configuration, please do confirm that Domain Computers is NOT denied.



Citrix FAS Administration Console - connected to localhost
Initial Setup
Rules
Advanced
Connect to another server
Refresh
Deploy
Publish
Reauthorize
Create
Connect

Complete these setup steps:

Deploy certificate templates

The required templates are deployed in Active Directory.

Set up a certificate authority

The authorization templates are published on: jackw-ad.xiaow.local\xiaow-jackw-ad-CA.

Click "Publish" to publish the templates on another certificate authority.

Authorize this service

An authorization certificate is configured.

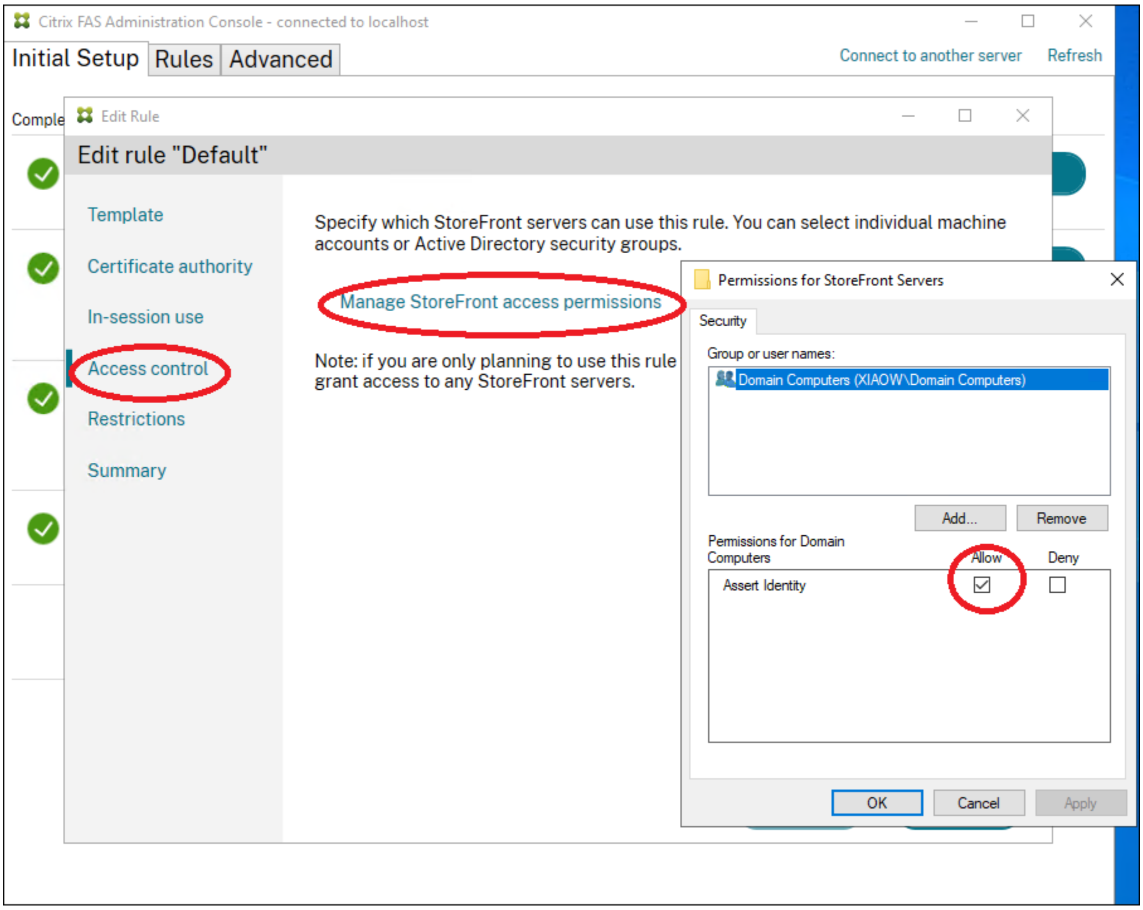
Deauthorize this service.

Create a rule

You have a rule configured: Default

Connect to Citrix Cloud

Complete this step if you wish to use this FAS service with Citrix Cloud.



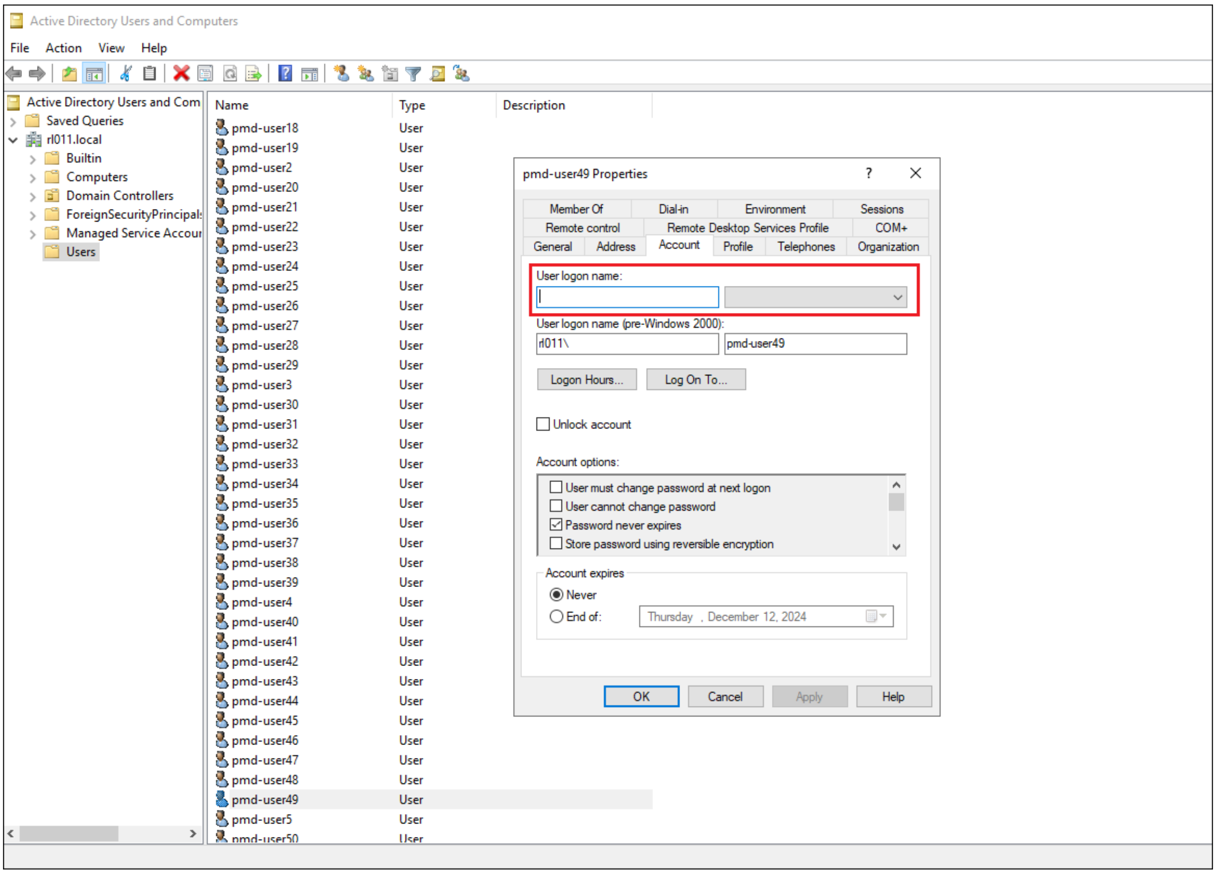
Citrix FAS Administration Console - connected to localhost
Initial Setup
Rules
Advanced
Connect to another server
Refresh
Comple
Edit Rule
Edit rule "Default"
Template
Certificate authority
In-session use
Access control
Restrictions
Summary
Manage StoreFront access permissions
Permissions for StoreFront Servers
Security
Group or user names:
Domain Computers (XIAOW\Domain Computers)
Add...
Remove
Permissions for Domain Computers
Allow
Deny
Assert Identity ☑ □
OK
Cancel
Apply

Specify which StoreFront servers can use this rule. You can select individual machine accounts or Active Directory security groups.

Note: if you are only planning to use this rule grant access to any StoreFront servers.

User Logon Name

For every end user, the **User logon name** must be configured.



Name	Type	Description
pmd-user18	User	
pmd-user19	User	
pmd-user2	User	
pmd-user20	User	
pmd-user21	User	
pmd-user22	User	
pmd-user23	User	
pmd-user24	User	
pmd-user25	User	
pmd-user26	User	
pmd-user27	User	
pmd-user28	User	
pmd-user29	User	
pmd-user3	User	
pmd-user30	User	
pmd-user31	User	
pmd-user32	User	
pmd-user33	User	
pmd-user34	User	
pmd-user35	User	
pmd-user36	User	
pmd-user37	User	
pmd-user38	User	
pmd-user39	User	
pmd-user4	User	
pmd-user40	User	
pmd-user41	User	
pmd-user42	User	
pmd-user43	User	
pmd-user44	User	
pmd-user45	User	
pmd-user46	User	
pmd-user47	User	
pmd-user48	User	
pmd-user49	User	
pmd-user5	User	
pmd-user50	User	

User logon name:

User logon name (pre-Windows 2000): rl011\ pmd-user49

□ Unlock account

Account options:

□ User must change password at next logon
□ User cannot change password
☑ Password never expires
□ Store password using reversible encryption

Account expires
● Never
○ End of: Thursday , December 12, 2024

Verify Session Remote Start API Calls

December 13, 2024

Enumeration and Launch

A sample script shall be provided to verify the installation, configuration, and API calls.

`enum_launch_example.ps1` (Only use the Citrix provided)

We strongly recommend executing the verification script on the 3rd-party Auth Service host.

The script enumerates and launches the resources by calling Session Remote Start APIs.

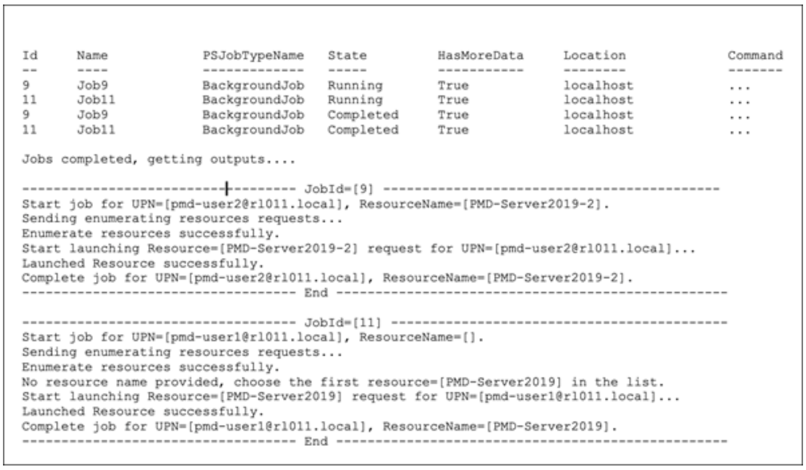
Run the script in PowerShell with two mandatory parameters:

- Fqdn: FQDN of the Session Remote Start server
- Upns: An array of UPNs and Resource Names separated by a colon (“:”), resource name can be omitted, in which case the first resource in the list is chosen.

Example:
`.\enum_launch_example.ps1 -Fqdn "pmd-server.rl011.local"-Upns "pmd-user2@rl011.local:PMD-Server2019-2","pmd-user1@rl011.local"`

In this example, the user **pmd-user2@rl011.local** is assigned to launch desktop **PMD-Server2019-2** (this is the name of the desktop as users see on their workspace). And no target resource is specified for user **pmd-user1@rl011.local**, the script will choose the first one in the resource list.

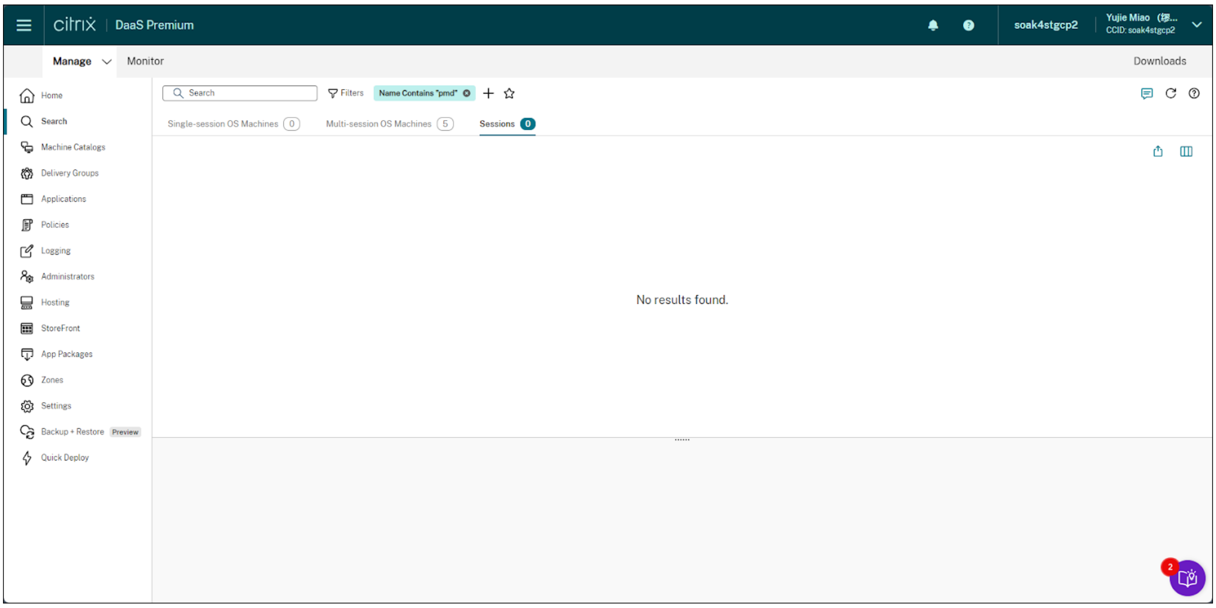
Output:



```
Id     Name            PSJobTypeName   State         HasMoreData     Location             Command
--     ----            -------------   -----         -----------     --------             -------
9      Job9            BackgroundJob   Running       True            localhost            ...
11     Job11           BackgroundJob   Running       True            localhost            ...
9      Job9            BackgroundJob   Completed     True            localhost            ...
11     Job11           BackgroundJob   Completed     True            localhost            ...

Jobs completed, getting outputs....

----------------------------------- JobId=[9] -------------------------------------------
Start job for UPN=[pmd-user2@rl011.local], ResourceName=[PMD-Server2019-2].
Sending enumerating resources requests...
Enumerate resources successfully.
Start launching Resource=[PMD-Server2019-2] request for UPN=[pmd-user2@rl011.local]...
Launched Resource successfully.
Complete job for UPN=[pmd-user2@rl011.local], ResourceName=[PMD-Server2019-2].
----------------------------------- End -------------------------------------------------

----------------------------------- JobId=[11] ------------------------------------------
Start job for UPN=[pmd-user1@rl011.local], ResourceName=[].
Sending enumerating resources requests...
Enumerate resources successfully.
No resource name provided, choose the first resource=[PMD-Server2019] in the list.
Start launching Resource=[PMD-Server2019] request for UPN=[pmd-user1@rl011.local]...
Launched Resource successfully.
Complete job for UPN=[pmd-user1@rl011.local], ResourceName=[PMD-Server2019].
----------------------------------- End -------------------------------------------------
```

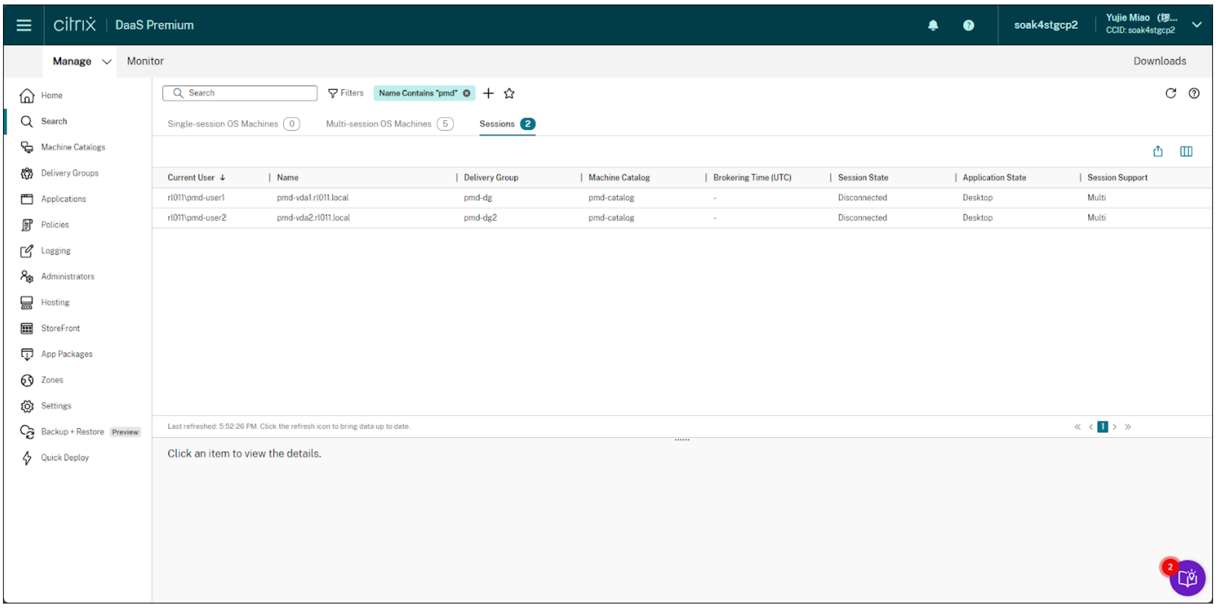
Verify the job output to make sure the resources are pre-launched successfully.

Alternatively, the execution result can be verified in Citrix Studio. Before running the script, no sessions are shown for the target machines:



No results found.

After running the script, the sessions are now shown to be in a disconnected state, which means the resources are prepared and ready to accept an incoming reconnect.



Current User	Name	Delivery Group	Machine Catalog	Brokering Time (UTC)	Session State	Application State	Session Support
rl011\pmd-user1	pmd-vda1.rl011.local	pmd-dg	pmd-catalog	-	Disconnected	Desktop	Multi
rl011\pmd-user2	pmd-vda2.rl011.local	pmd-dg2	pmd-catalog	-	Disconnected	Desktop	Multi

Last refreshed: 5:52:26 PM. Click the refresh icon to bring data up to date.

Click an item to view the details.

Logoff

logoff_example.ps1 (Only use the Citrix provided)

The script logoffs the resources by calling Session Remote Start APIs.

Run the script in PowerShell with two mandatory parameters:

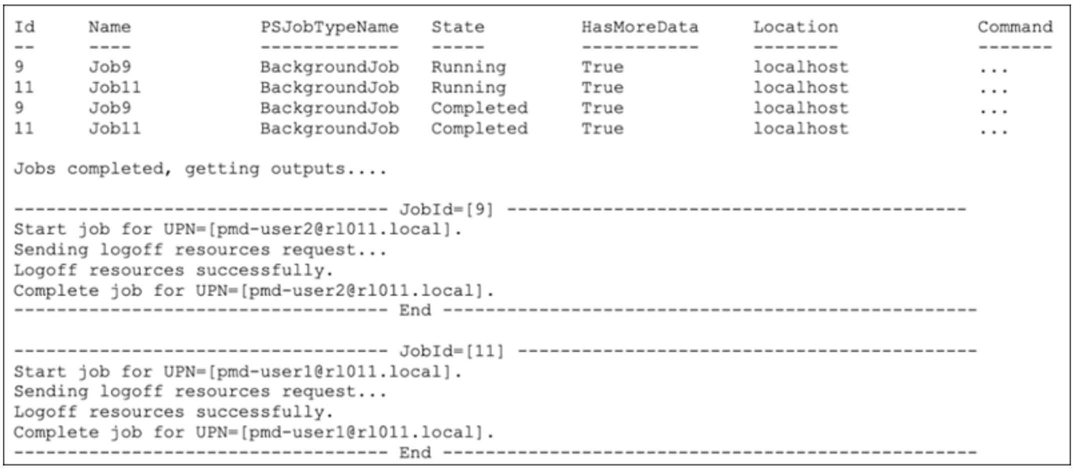
- Fqdn: FQDN of the Session Remote Start server
- Upns: An array of UPNs.

Example:

```
.\logoff_example.ps1 -Fqdn "pmd-server.rl011.local"-Upns "pmd-user2@rl011
.local","pmd-user1@rl011.local"
```

In this example, the script will logoff all the resources for the users **pmd-user2@rl011.local** and **pmd-user1@rl011.local**.

Output:



```
Id     Name            PSJobTypeName   State         HasMoreData     Location             Command
--     ----            -------------   -----         -----------     --------             -------
9      Job9            BackgroundJob   Running       True            localhost            ...
11     Job11           BackgroundJob   Running       True            localhost            ...
9      Job9            BackgroundJob   Completed     True            localhost            ...
11     Job11           BackgroundJob   Completed     True            localhost            ...

Jobs completed, getting outputs....

----------------------------------- JobId=[9] -------------------------------------------
Start job for UPN=[pmd-user2@r1011.local].
Sending logoff resources request...
Logoff resources successfully.
Complete job for UPN=[pmd-user2@r1011.local].
----------------------------------- End --------------------------------------------------

----------------------------------- JobId=[11] ------------------------------------------
Start job for UPN=[pmd-user1@r1011.local].
Sending logoff resources request...
Logoff resources successfully.
Complete job for UPN=[pmd-user1@r1011.local].
----------------------------------- End --------------------------------------------------
```

> Note:
>
> This API simply issues the log off request and does not wait for the sessions to complete logging off.

Session Remote Start local testing

January 15, 2025

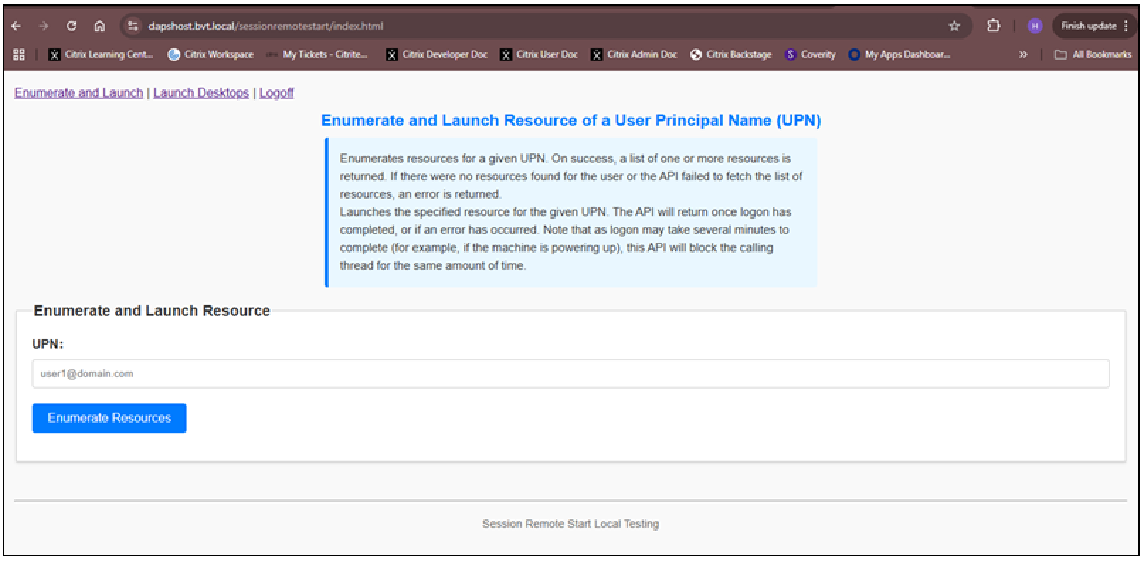
Open Session Remote Start Web Local Testing

Open `https://<Session Remote Start FQDN>/SessionRemoteStart/index.html`, if successful without warning. There are three tabs on the top left: **Enumerate and Launch**, **Launch Desktops**, and **Logoff**.

1. **Enumerate and Launch**: Enumerate resources for a given UPN. Then launch the specified resource for the given UPN.
2. **Launch Desktops**: Session Remote Start supports launching all desktops using three methods.

    - Launch All Desktops of a User Principal Name (UPN)
    - Launch All Desktops by Tags of a User Principal Name (UPN)
    - Launch All Desktops assigned to the UPNs in the specified AD groups

3. **Logoff**: Logs off all sessions for the given UPN and device name.



Enumerate and Launch | Launch Desktops | Logoff

Enumerate and Launch Resource of a User Principal Name (UPN)

Enumerates resources for a given UPN. On success, a list of one or more resources is returned. If there were no resources found for the user or the API failed to fetch the list of resources, an error is returned.
Launches the specified resource for the given UPN. The API will return once logon has completed, or if an error has occurred. Note that as logon may take several minutes to complete (for example, if the machine is powering up), this API will block the calling thread for the same amount of time.

Enumerate and Launch Resource

UPN:

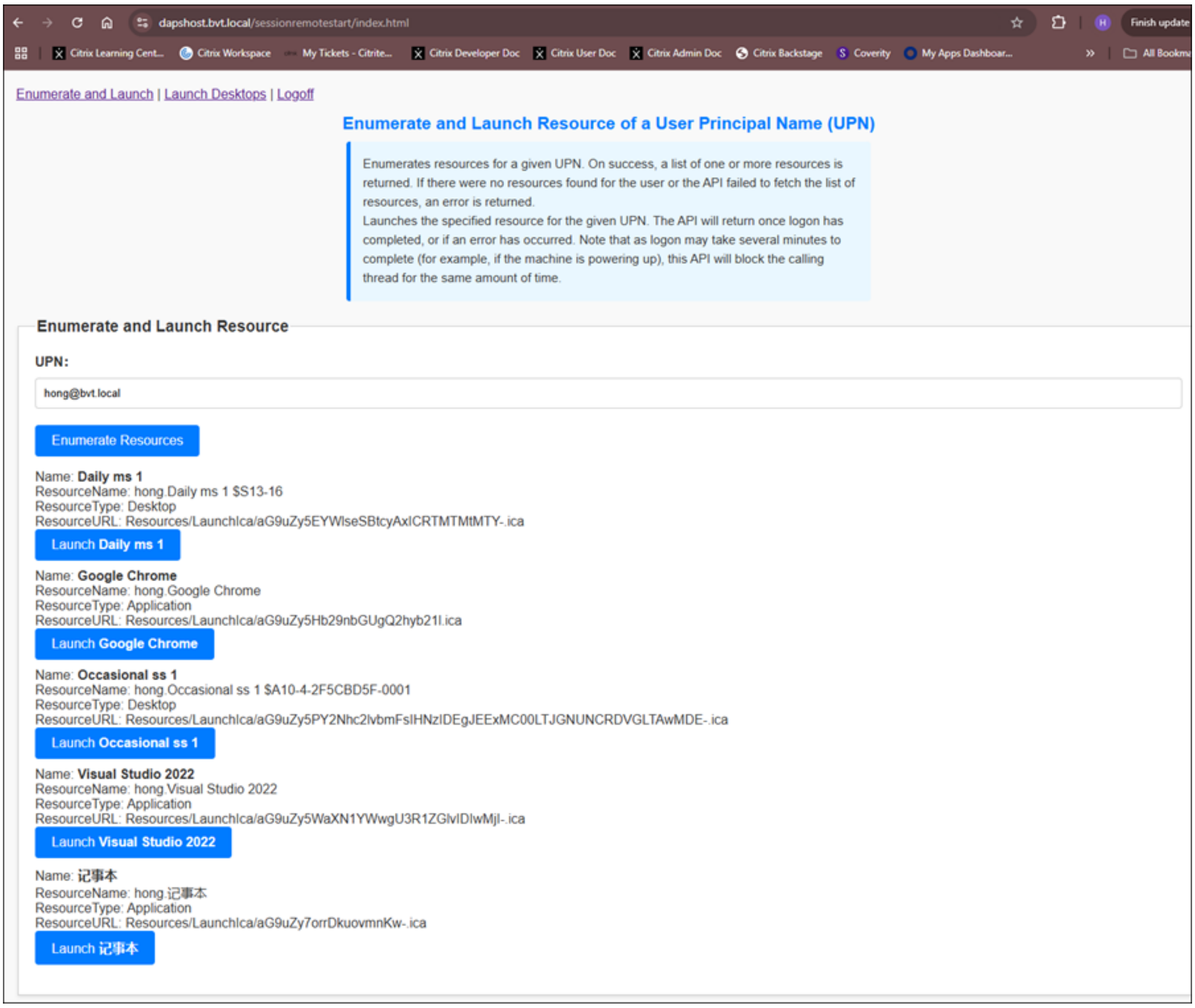
user1@domain.com

Enumerate Resources

Session Remote Start Local Testing

Enumerate and Launch Resource of a User Principal Name (UPN)

Input the User Principal Name (UPN), then click **Enumerate Resources**.



Enumerate and Launch | Launch Desktops | Logoff

Enumerate and Launch Resource of a User Principal Name (UPN)

Enumerates resources for a given UPN. On success, a list of one or more resources is returned. If there were no resources found for the user or the API failed to fetch the list of resources, an error is returned.
Launches the specified resource for the given UPN. The API will return once logon has completed, or if an error has occurred. Note that as logon may take several minutes to complete (for example, if the machine is powering up), this API will block the calling thread for the same amount of time.

Enumerate and Launch Resource

UPN:

hong@bvt.local

Name: **Daily ms 1**
ResourceName: hong.Daily ms 1 $S13-16
ResourceType: Desktop
ResourceURL: Resources/LaunchIca/aG9uZy5EYWlseSBtcyAxICRTMTMtMTY-.ica

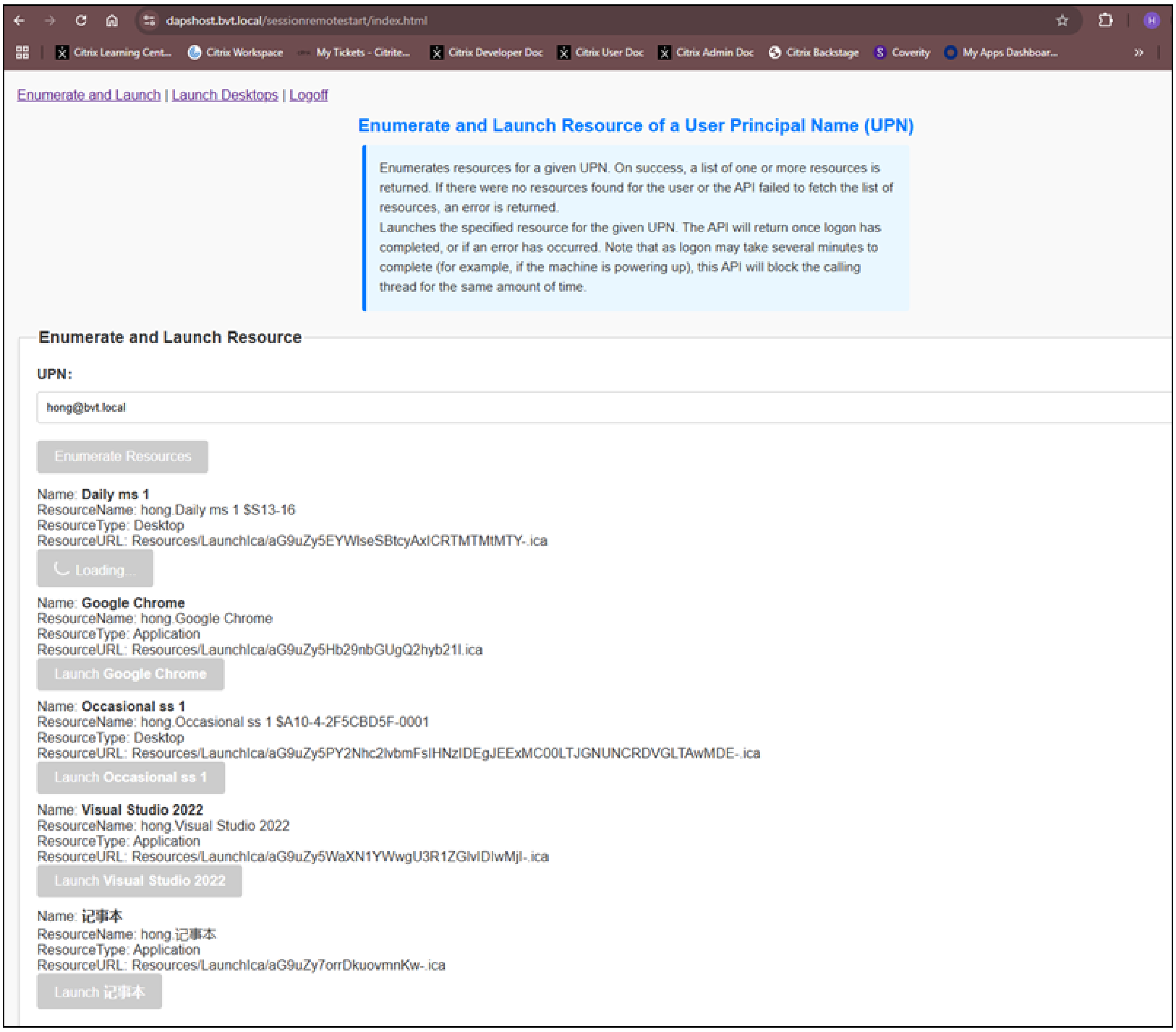
Name: **Google Chrome**
ResourceName: hong.Google Chrome
ResourceType: Application
ResourceURL: Resources/LaunchIca/aG9uZy5Hb29nbGUgQ2hyb21l.ica

Name: **Occasional ss 1**
ResourceName: hong.Occasional ss 1 $A10-4-2F5CBD5F-0001
ResourceType: Desktop
ResourceURL: Resources/LaunchIca/aG9uZy5PY2Nhc2lvbmFsIHNzIDEgJEExMC00LTJGNUNCRDVGLTAwMDE-.ica

Name: **Visual Studio 2022**
ResourceName: hong.Visual Studio 2022
ResourceType: Application
ResourceURL: Resources/LaunchIca/aG9uZy5WaXN1YWwgU3R1ZGlvIDIwMjI-.ica

Name: **记事本**
ResourceName: hong.记事本
ResourceType: Application
ResourceURL: Resources/LaunchIca/aG9uZy7orrDkuovmnKw-.ica

Then choose a resource, for example: `Daily ms 1` and click `Launch Daily ms 1`. The API waits for a logon notification from the VDA before returning to the caller.



Enumerate and Launch | Launch Desktops | Logoff

Enumerate and Launch Resource of a User Principal Name (UPN)

Enumerates resources for a given UPN. On success, a list of one or more resources is returned. If there were no resources found for the user or the API failed to fetch the list of resources, an error is returned.
Launches the specified resource for the given UPN. The API will return once logon has completed, or if an error has occurred. Note that as logon may take several minutes to complete (for example, if the machine is powering up), this API will block the calling thread for the same amount of time.

Enumerate and Launch Resource

UPN:

hong@bvt.local

Name: **Daily ms 1**
ResourceName: hong.Daily ms 1 $S13-16
ResourceType: Desktop
ResourceURL: Resources/LaunchIca/aG9uZy5EYWlseSBtcyAxICRTMTMtMTY-.ica

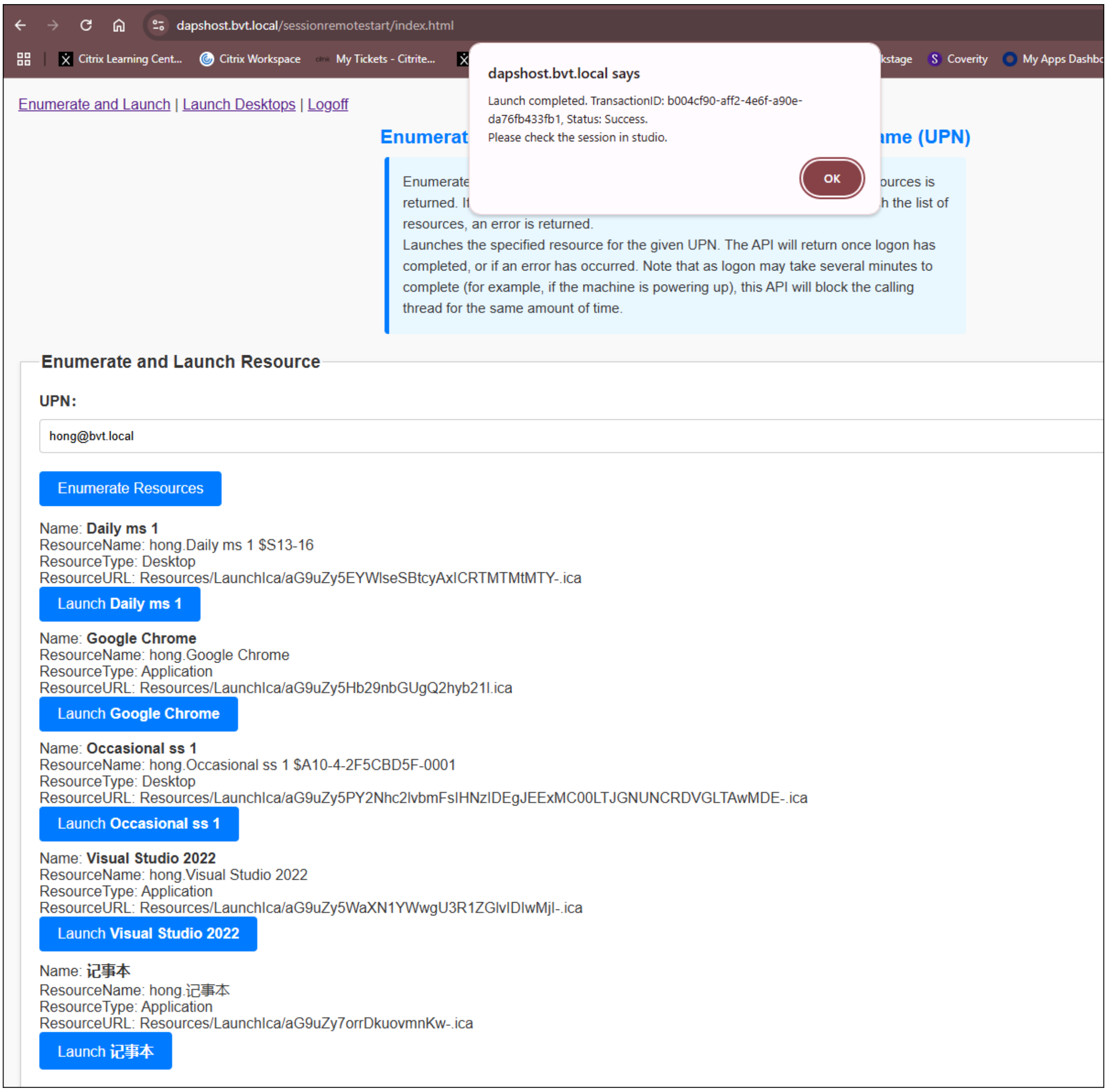
Name: **Google Chrome**
ResourceName: hong.Google Chrome
ResourceType: Application
ResourceURL: Resources/LaunchIca/aG9uZy5Hb29nbGUgQ2hyb21l.ica

Name: **Occasional ss 1**
ResourceName: hong.Occasional ss 1 $A10-4-2F5CBD5F-0001
ResourceType: Desktop
ResourceURL: Resources/LaunchIca/aG9uZy5PY2Nhc2lvbmFsIHNzIDEgJEExMC00LTJGNUNCRDVGLTAwMDE-.ica

Name: **Visual Studio 2022**
ResourceName: hong.Visual Studio 2022
ResourceType: Application
ResourceURL: Resources/LaunchIca/aG9uZy5WaXN1YWwgU3R1ZGlvIDIwMjI-.ica

Name: **记事本**
ResourceName: hong.记事本
ResourceType: Application
ResourceURL: Resources/LaunchIca/aG9uZy7orrDkuovmnKw-.ica

A prompt appears with a notification if the resource is launched successfully. Then, check the session in the studio.



dapshost.bvt.local/sessionremotestart/index.html
Citrix Learning Cent...
Citrix Workspace
My Tickets - Citrite...
kstage
Coverity
My Apps Dashbc

dapshost.bvt.local says

Launch completed. TransactionID: b004cf90-aff2-4e6f-a90e-da76fb433fb1, Status: Success.
Please check the session in studio.

Enumerate and Launch | Launch Desktops | Logoff

Enumerat ame (UPN)

Enumerate ources is returned. If h the list of resources, an error is returned.
Launches the specified resource for the given UPN. The API will return once logon has completed, or if an error has occurred. Note that as logon may take several minutes to complete (for example, if the machine is powering up), this API will block the calling thread for the same amount of time.

Enumerate and Launch Resource

UPN: hong@bvt.local

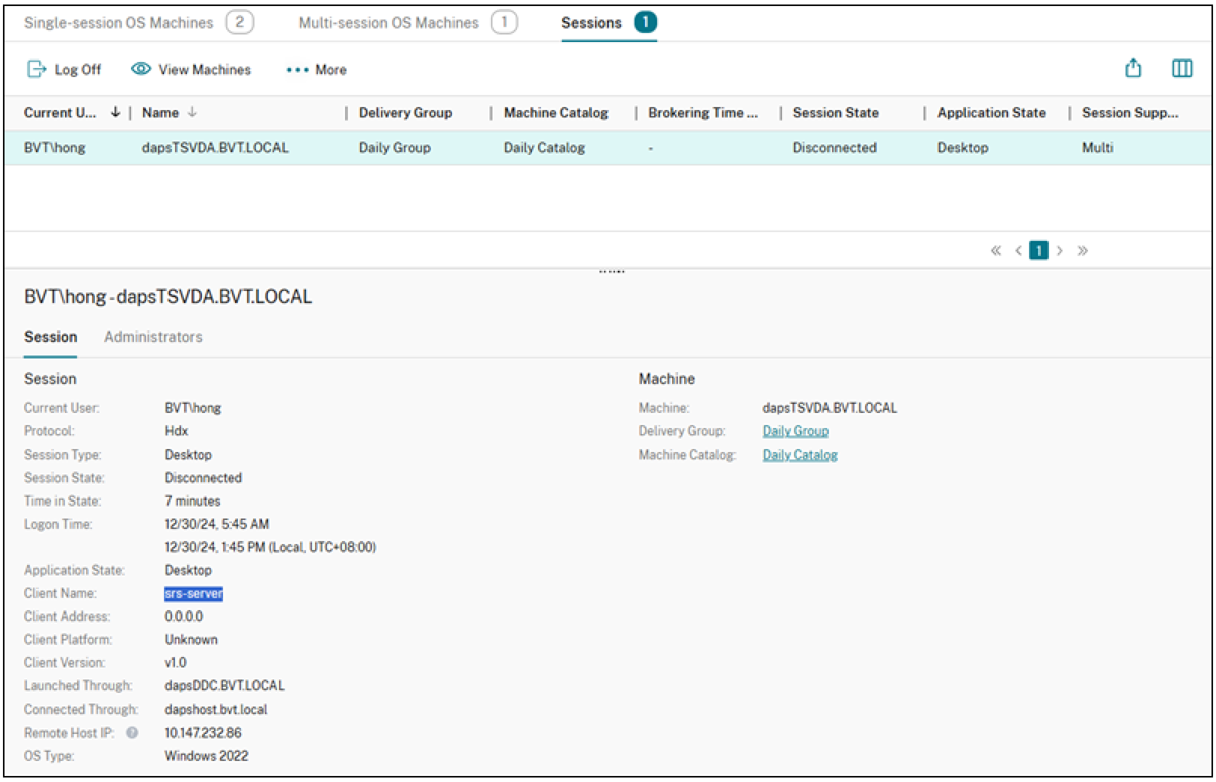
Name: **Daily ms 1**
ResourceName: hong.Daily ms 1 $S13-16
ResourceType: Desktop
ResourceURL: Resources/LaunchIca/aG9uZy5EYWlseSBtcyAxICRTMTMtMTY-.ica

Name: **Google Chrome**
ResourceName: hong.Google Chrome
ResourceType: Application
ResourceURL: Resources/LaunchIca/aG9uZy5Hb29nbGUgQ2hyb21l.ica

Name: **Occasional ss 1**
ResourceName: hong.Occasional ss 1 $A10-4-2F5CBD5F-0001
ResourceType: Desktop
ResourceURL: Resources/LaunchIca/aG9uZy5PY2Nhc2lvbmFsIHNzIDEgJEExMC00LTJGNUNCRDVGLTAwMDE-.ica

Name: **Visual Studio 2022**
ResourceName: hong.Visual Studio 2022
ResourceType: Application
ResourceURL: Resources/LaunchIca/aG9uZy5WaXN1YWwgU3R1ZGlvIDIwMjI-.ica

Name: **记事本**
ResourceName: hong.记事本
ResourceType: Application
ResourceURL: Resources/LaunchIca/aG9uZy7orrDkuovmnKw-.ica



Current U...	Name	Delivery Group	Machine Catalog	Brokering Time ...	Session State	Application State	Session Supp...
BVT\hong	dapsTSVDA.BVT.LOCAL	Daily Group	Daily Catalog	-	Disconnected	Desktop	Multi

BVT\hong - dapsTSVDA.BVT.LOCAL

Session

Current User:	BVT\hong
Protocol:	Hdx
Session Type:	Desktop
Session State:	Disconnected
Time in State:	7 minutes
Logon Time:	12/30/24, 5:45 AM 12/30/24, 1:45 PM (Local, UTC+08:00)
Application State:	Desktop
Client Name:	srs-server
Client Address:	0.0.0.0
Client Platform:	Unknown
Client Version:	v1.0
Launched Through:	dapsDDC.BVT.LOCAL
Connected Through:	dapshost.bvt.local
Remote Host IP:	10.147.232.86
OS Type:	Windows 2022

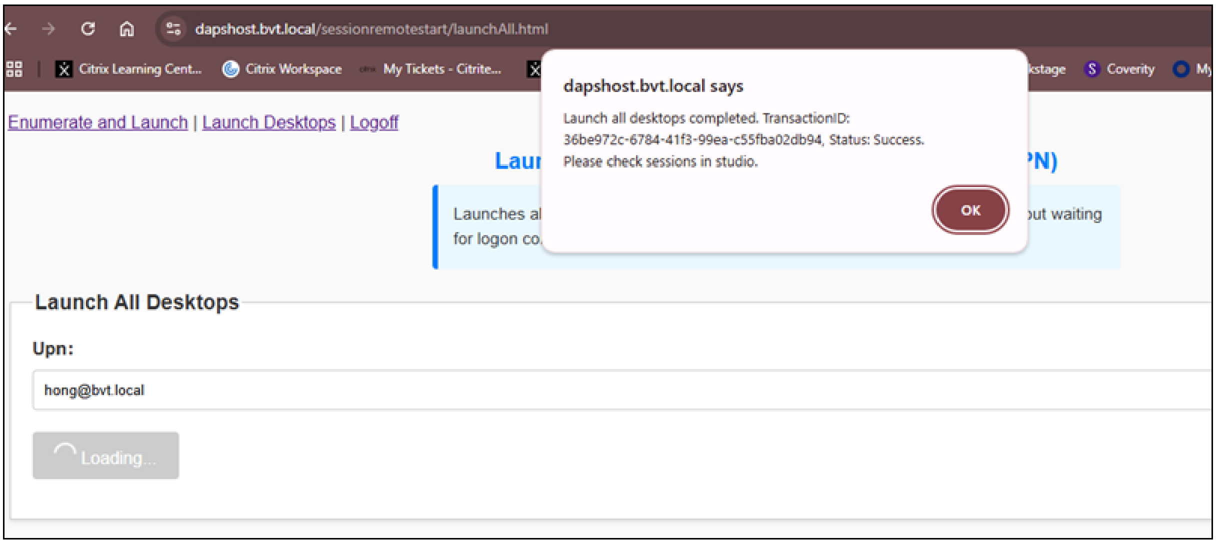
Machine

Machine:	dapsTSVDA.BVT.LOCAL
Delivery Group:	Daily Group
Machine Catalog:	Daily Catalog

Launch Desktops

Launch All Desktops of a User Principal Name (UPN)

Enter the User Principal Name (UPN), then click **Launch All Desktops**. A prompt appears with a notification if the resources are launched successfully. Then, check the sessions in the studio.

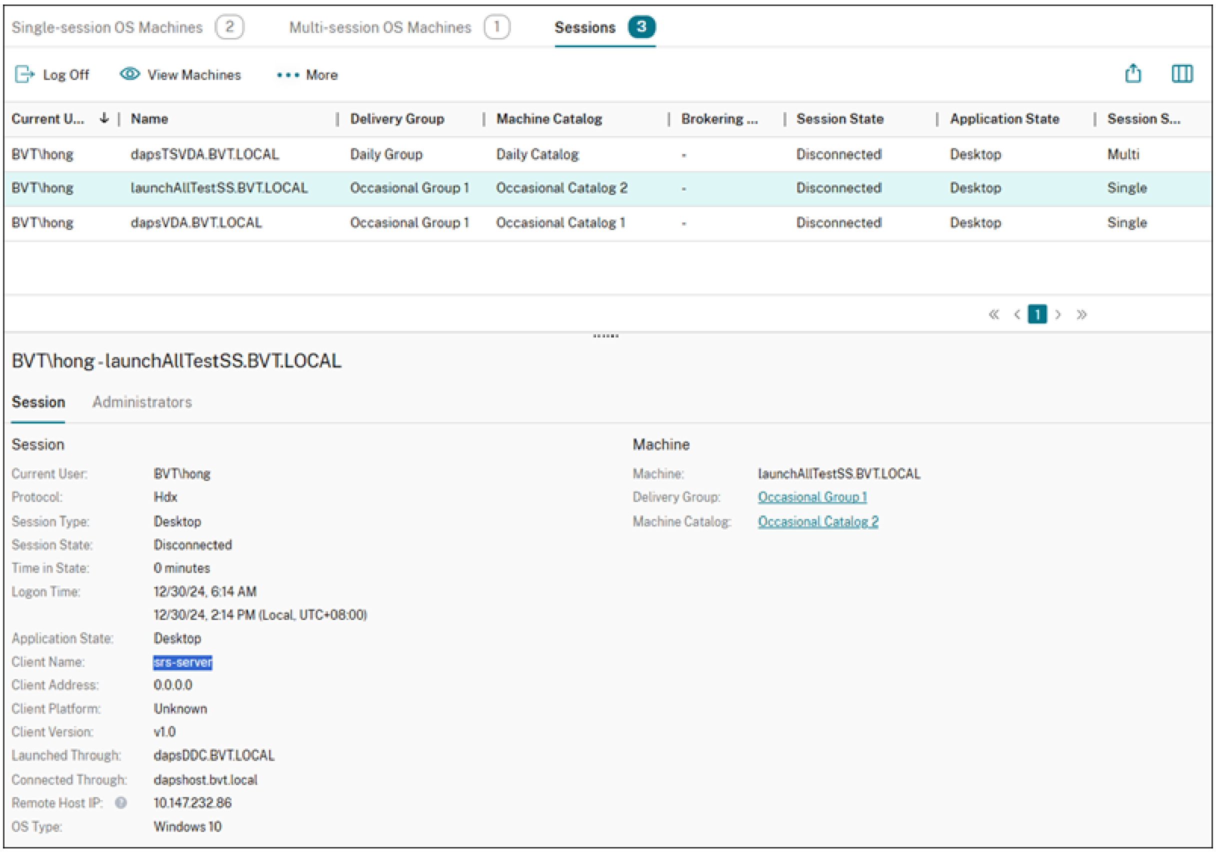


dapshost.bvt.local says

Launch all desktops completed. TransactionID: 36be972c-6784-41f3-99ea-c55fba02db94, Status: Success. Please check sessions in studio.

Launch All Desktops

Upn: hong@bvt.local



Current U...	Name	Delivery Group	Machine Catalog	Brokering ...	Session State	Application State	Session S...
BVT\hong	dapsTSVDA.BVT.LOCAL	Daily Group	Daily Catalog	-	Disconnected	Desktop	Multi
BVT\hong	launchAllTestSS.BVT.LOCAL	Occasional Group 1	Occasional Catalog 2	-	Disconnected	Desktop	Single
BVT\hong	dapsVDA.BVT.LOCAL	Occasional Group 1	Occasional Catalog 1	-	Disconnected	Desktop	Single

BVT\hong - launchAllTestSS.BVT.LOCAL

Session | Administrators

Session

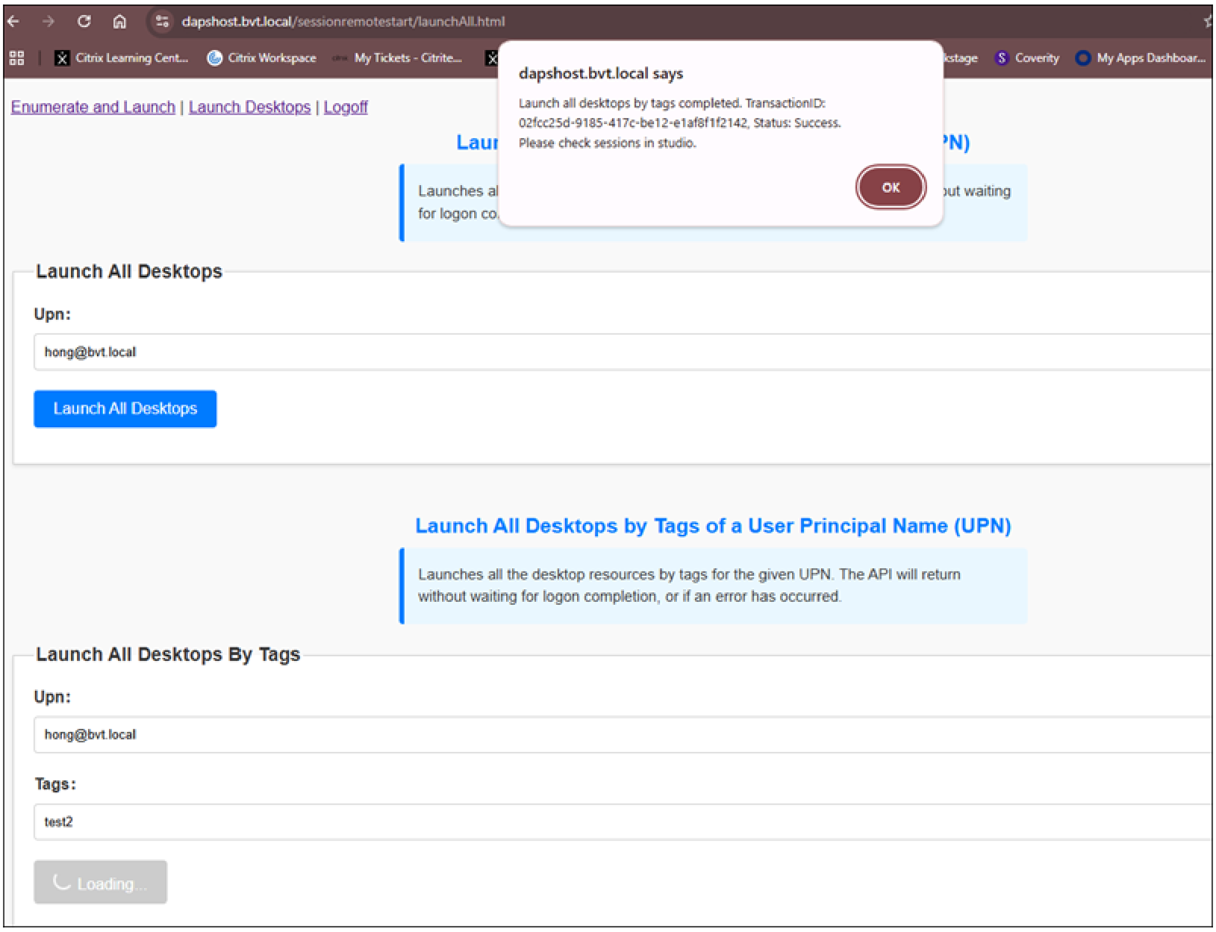
Current User:	BVT\hong
Protocol:	Hdx
Session Type:	Desktop
Session State:	Disconnected
Time in State:	0 minutes
Logon Time:	12/30/24, 6:14 AM 12/30/24, 2:14 PM (Local, UTC+08:00)
Application State:	Desktop
Client Name:	srs-server
Client Address:	0.0.0.0
Client Platform:	Unknown
Client Version:	v1.0
Launched Through:	dapsDDC.BVT.LOCAL
Connected Through:	dapshost.bvt.local
Remote Host IP:	10.147.232.86
OS Type:	Windows 10

Machine

Machine:	launchAllTestSS.BVT.LOCAL
Delivery Group:	Occasional Group 1
Machine Catalog:	Occasional Catalog 2

Launch All Desktops by Tags of a User Principal Name (UPN)

Enter the User Principal Name (UPN) and tags, then click **Launch All Desktops By Tags**. A prompt appears with a notification if the resources are launched successfully. Then, check the sessions in the studio.



dapshost.bvt.local says

Launch all desktops by tags completed. TransactionID: 02fcc25d-9185-417c-be12-e1af8f1f2142, Status: Success. Please check sessions in studio.

Launches al... for logon co... ...out waiting

Launch All Desktops

Upn: hong@bvt.local

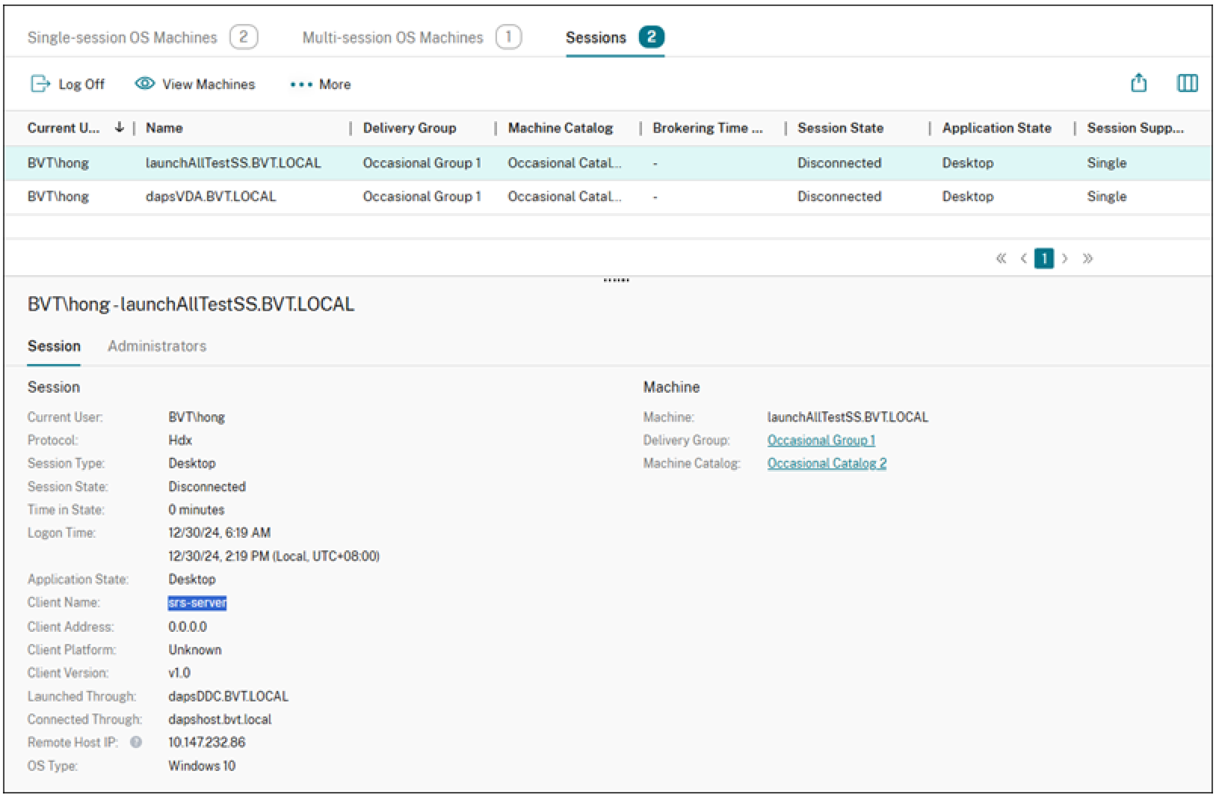
Launch All Desktops by Tags of a User Principal Name (UPN)

Launches all the desktop resources by tags for the given UPN. The API will return without waiting for logon completion, or if an error has occurred.

Launch All Desktops By Tags

Upn: hong@bvt.local

Tags: test2



Current U...	Name	Delivery Group	Machine Catalog	Brokering Time ...	Session State	Application State	Session Supp...
BVT\hong	launchAllTestSS.BVT.LOCAL	Occasional Group 1	Occasional Catal...	-	Disconnected	Desktop	Single
BVT\hong	dapsVDA.BVT.LOCAL	Occasional Group 1	Occasional Catal...	-	Disconnected	Desktop	Single

BVT\hong - launchAllTestSS.BVT.LOCAL

Session

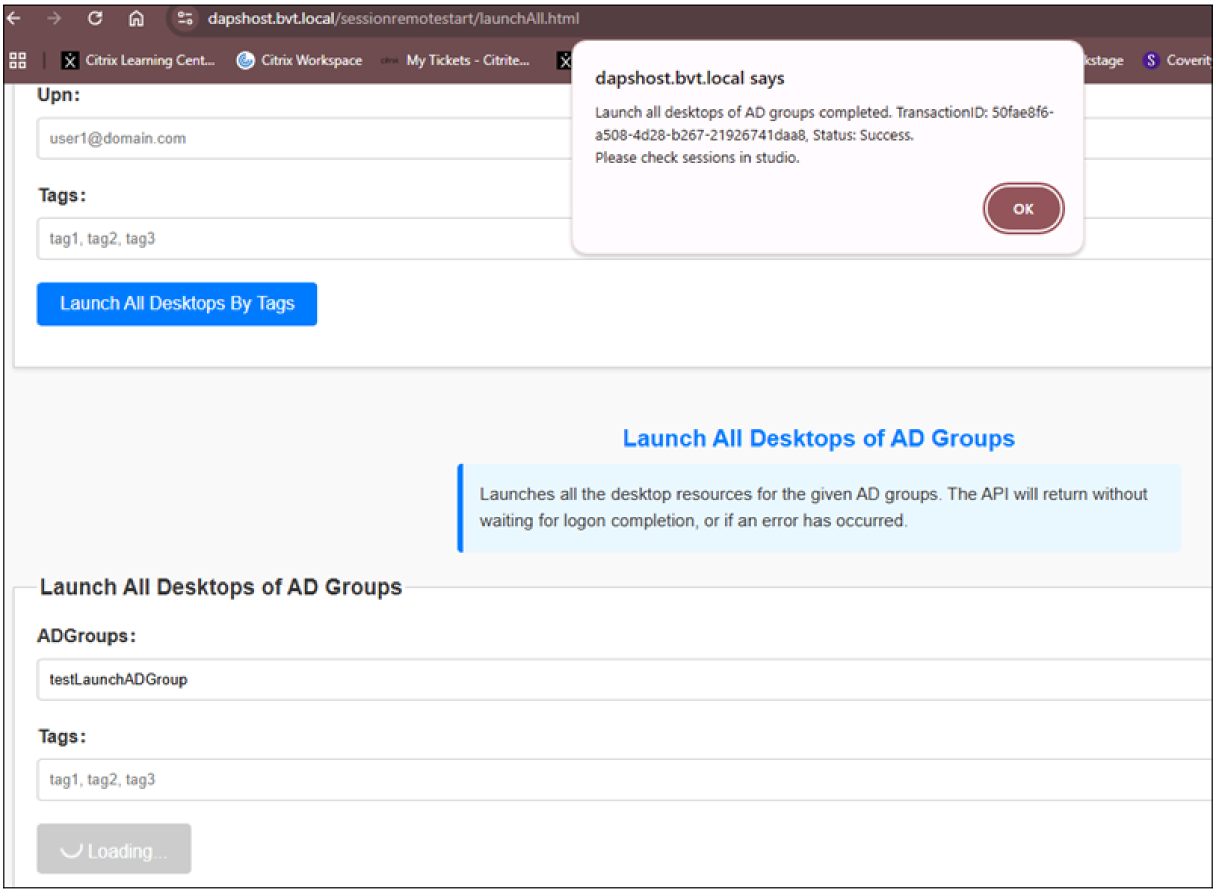
Current User:	BVT\hong
Protocol:	Hdx
Session Type:	Desktop
Session State:	Disconnected
Time in State:	0 minutes
Logon Time:	12/30/24, 6:19 AM 12/30/24, 2:19 PM (Local, UTC+08:00)
Application State:	Desktop
Client Name:	srs-server
Client Address:	0.0.0.0
Client Platform:	Unknown
Client Version:	v1.0
Launched Through:	dapsDDC.BVT.LOCAL
Connected Through:	dapshost.bvt.local
Remote Host IP:	10.147.232.86
OS Type:	Windows 10

Machine

Machine:	launchAllTestSS.BVT.LOCAL
Delivery Group:	Occasional Group 1
Machine Catalog:	Occasional Catalog 2

Launch All Desktops of AD Groups

Input AD Groups then click **Launch All Desktops of AD Groups**. A prompt appears with a notification if the resources are launched successfully. Then, check the sessions in the studio.



dapshost.bvt.local says

Launch all desktops of AD groups completed. TransactionID: 50fae8f6-a508-4d28-b267-21926741daa8, Status: Success.
Please check sessions in studio.

OK

Upn: user1@domain.com

Tags: tag1, tag2, tag3

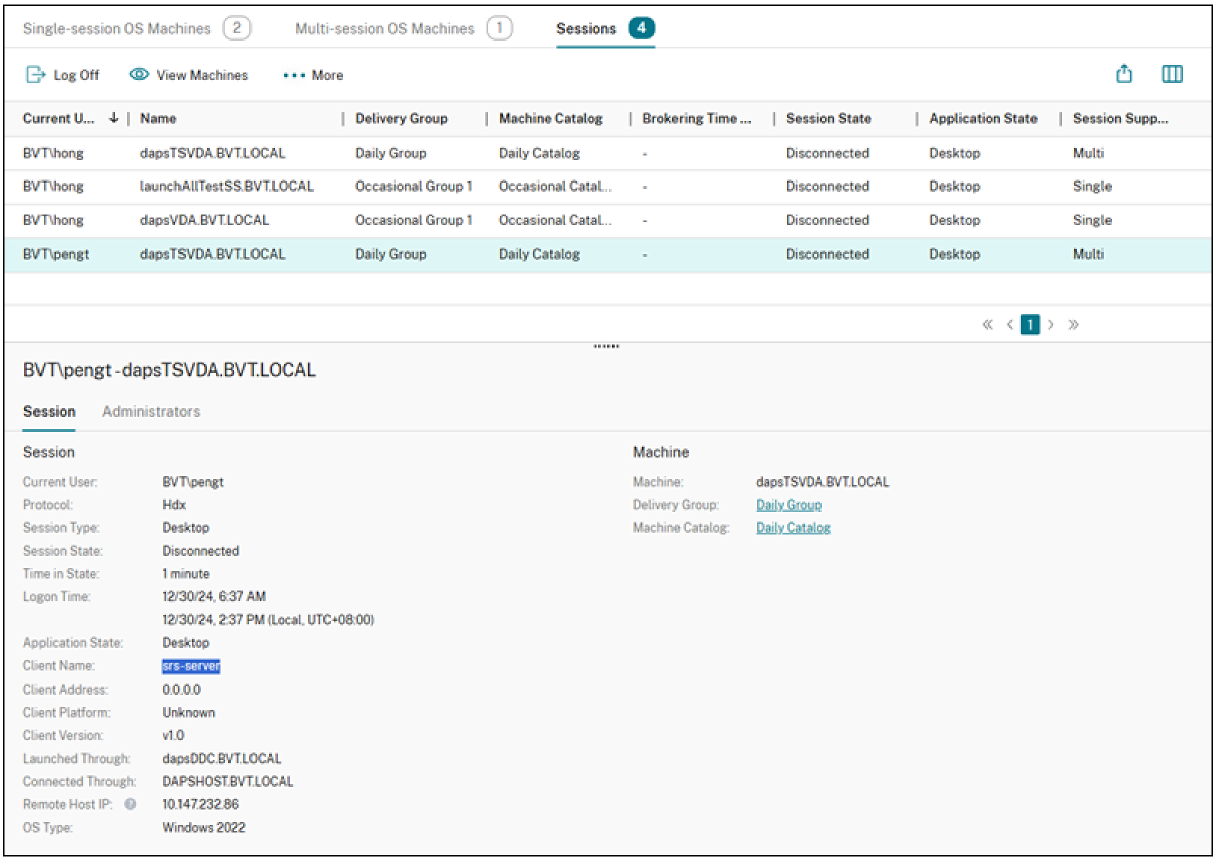
Launch All Desktops of AD Groups

Launches all the desktop resources for the given AD groups. The API will return without waiting for logon completion, or if an error has occurred.

Launch All Desktops of AD Groups

ADGroups: testLaunchADGroup

Tags: tag1, tag2, tag3



Current U...	Name	Delivery Group	Machine Catalog	Brokering Time ...	Session State	Application State	Session Supp...
BVT\hong	dapsTSVDA.BVT.LOCAL	Daily Group	Daily Catalog	-	Disconnected	Desktop	Multi
BVT\hong	launchAllTestSS.BVT.LOCAL	Occasional Group 1	Occasional Catal...	-	Disconnected	Desktop	Single
BVT\hong	dapsVDA.BVT.LOCAL	Occasional Group 1	Occasional Catal...	-	Disconnected	Desktop	Single
BVT\pengt	dapsTSVDA.BVT.LOCAL	Daily Group	Daily Catalog	-	Disconnected	Desktop	Multi

BVT\pengt - dapsTSVDA.BVT.LOCAL

Session

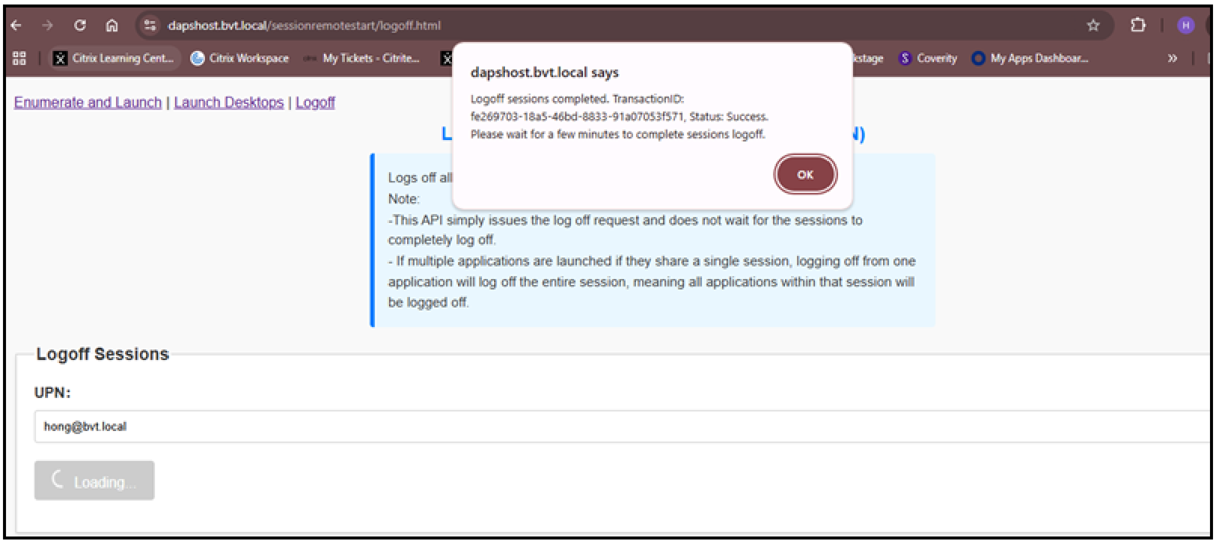
Current User: BVT\pengt
Protocol: Hdx
Session Type: Desktop
Session State: Disconnected
Time in State: 1 minute
Logon Time: 12/30/24, 6:37 AM
12/30/24, 2:37 PM (Local, UTC+08:00)
Application State: Desktop
Client Name: srs-server
Client Address: 0.0.0.0
Client Platform: Unknown
Client Version: v1.0
Launched Through: dapsDDC.BVT.LOCAL
Connected Through: DAPSHOST.BVT.LOCAL
Remote Host IP: 10.147.232.86
OS Type: Windows 2022

Machine

Machine: dapsTSVDA.BVT.LOCAL
Delivery Group: Daily Group
Machine Catalog: Daily Catalog

Log off Sessions of a User Principal Name (UPN)

Input the User Principal Name (UPN), then click **Logoff Sessions**. A prompt appears with a notification if the sessions are logoff successfully. Then, check the sessions in the studio.



dapshost.bvt.local says

Logoff sessions completed. TransactionID: fe269703-18a5-46bd-8833-91a07053f571, Status: Success. Please wait for a few minutes to complete sessions logoff.

Logs off all

Note:

-This API simply issues the log off request and does not wait for the sessions to completely log off.

- If multiple applications are launched if they share a single session, logging off from one application will log off the entire session, meaning all applications within that session will be logged off.

Logoff Sessions

UPN: hong@bvt.local

Verify Session Remote Start API Calls

Enumeration and Launch

A sample script is provided to verify the installation, configuration, and API calls.

`enum_launch_example.ps1` (Use the one provided by Citrix)

We strongly recommend running the verification script on the 3rd-party Auth Service host.

The script enumerates and launches the resources by calling the Session Remote Start APIs.

Run the script in PowerShell with two mandatory parameters:

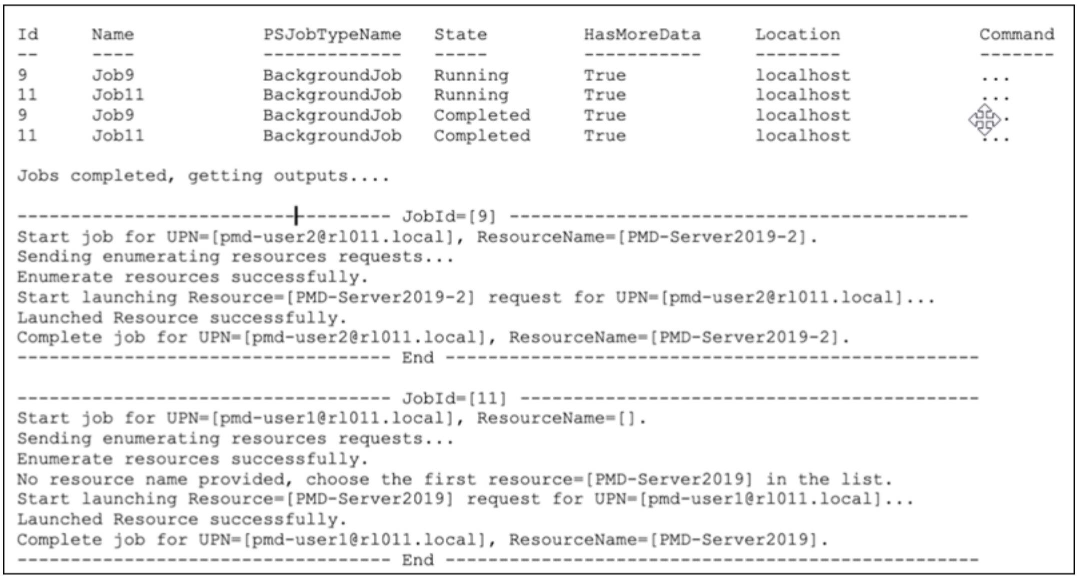
- Fqdn: FQDN of the Session Remote Start server
- Upns: An array of UPNs and Resource Names separated by a colon (":"), resource name can be omitted, in which case the first resource in the list will be chosen.

Example:

```
.\enum_launch_example.ps1 -Fqdn "pmd-server.rl011.local"-Upns "pmd-user2@rl011.local:PMD-Server2019-2","pmd-user1@rl011.local"
```

In this example, the user `"pmd-user2@rl011.local"` is assigned to launch desktop `"PMD-Server2019-2"` (this is the name of the desktop as users see on their workspace). And no target resource is specified for user `"pmd-user1@rl011.local"`. The script chooses the first one in the resource list.

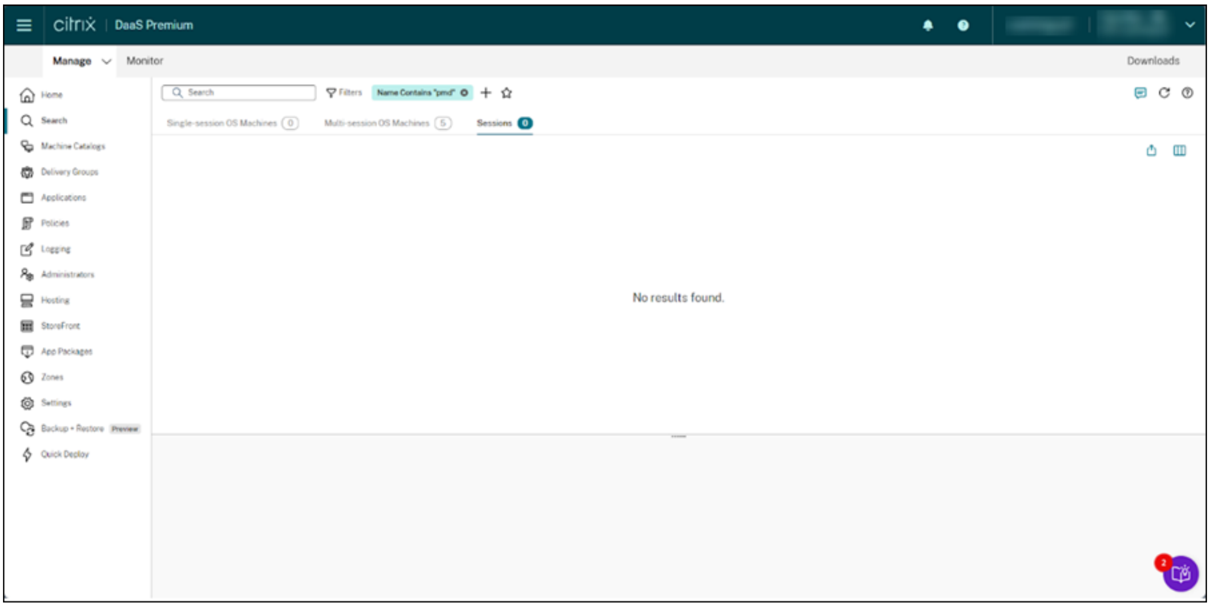
Output:



```
Id     Name            PSJobTypeName   State         HasMoreData     Location             Command
--     ----            -------------   -----         -----------     --------             -------
9      Job9            BackgroundJob   Running       True            localhost            ...
11     Job11           BackgroundJob   Running       True            localhost            ...
9      Job9            BackgroundJob   Completed     True            localhost            ...
11     Job11           BackgroundJob   Completed     True            localhost            ...

Jobs completed, getting outputs....

----------------------------------- JobId=[9] --------------------------------------------
Start job for UPN=[pmd-user2@rl011.local], ResourceName=[PMD-Server2019-2].
Sending enumerating resources requests...
Enumerate resources successfully.
Start launching Resource=[PMD-Server2019-2] request for UPN=[pmd-user2@rl011.local]...
Launched Resource successfully.
Complete job for UPN=[pmd-user2@rl011.local], ResourceName=[PMD-Server2019-2].
----------------------------------- End --------------------------------------------------

----------------------------------- JobId=[11] -------------------------------------------
Start job for UPN=[pmd-user1@rl011.local], ResourceName=[].
Sending enumerating resources requests...
Enumerate resources successfully.
No resource name provided, choose the first resource=[PMD-Server2019] in the list.
Start launching Resource=[PMD-Server2019] request for UPN=[pmd-user1@rl011.local]...
Launched Resource successfully.
Complete job for UPN=[pmd-user1@rl011.local], ResourceName=[PMD-Server2019].
----------------------------------- End --------------------------------------------------
```

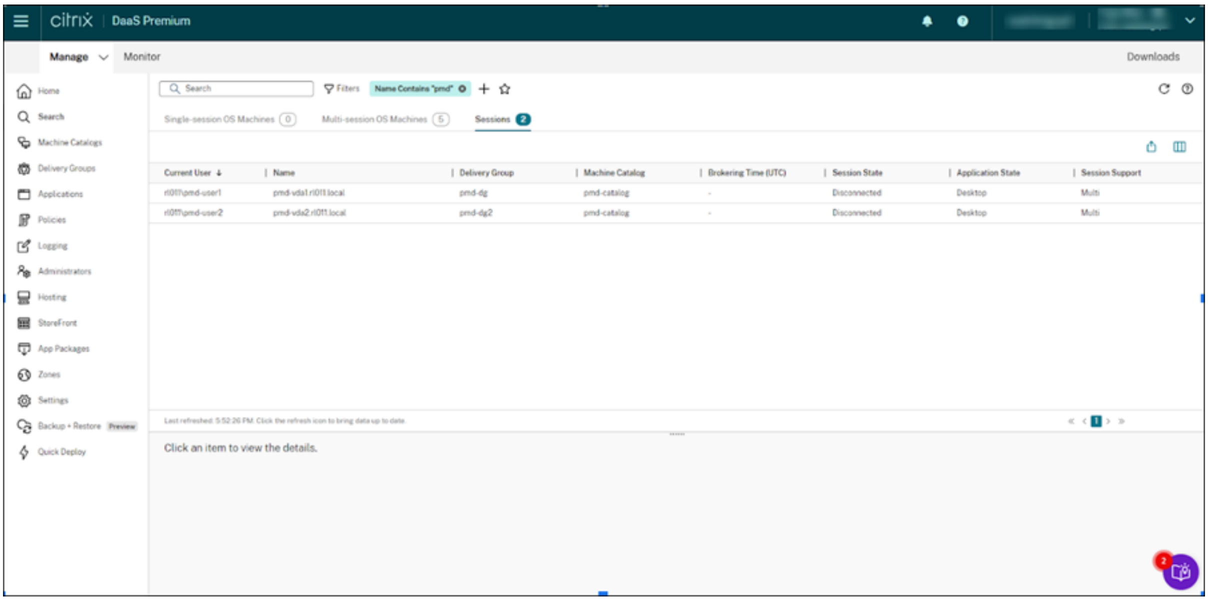
Verify the job output to make sure the resources are pre-launched successfully.

Alternatively, the execution result can be verified in Citrix Studio. Before running the script, no sessions are shown for the target machines:



No results found.

After running the script, the sessions are shown in a disconnected state, which means the resources are prepared and ready to accept an incoming reconnect.



Current User	Name	Delivery Group	Machine Catalog	Brokering Time (UTC)	Session State	Application State	Session Support
rl011\pmd-user1	pmd-vda1.rl011.local	pmd-dg	pmd-catalog	-	Disconnected	Desktop	Multi
rl011\pmd-user2	pmd-vda2.rl011.local	pmd-dg2	pmd-catalog	-	Disconnected	Desktop	Multi

Last refreshed: 5:52:26 PM. Click the refresh icon to bring data up to date.

Click an item to view the details.

Logoff

`logoff_example.ps1` (Please use the one provided by Citrix)

The script logs off the resources by calling the Session Remote Start APIs.

Run the script in PowerShell with two mandatory parameters:

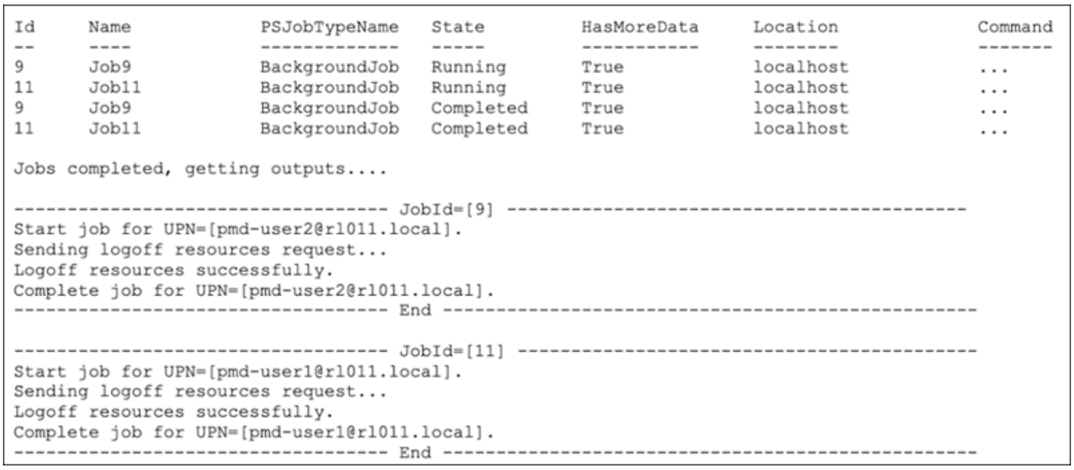
- Fqdn: FQDN of the Session Remote Start server
- Puns: An array of UPNs.

Example:

```
.\logoff_example.ps1 -Fqdn "pmd-server.rl011.local"-Upns "pmd-user2@rl011
.local","pmd-user1@rl011.local"
```

In this example, the script log off all the resources for the users `"pmd-user2@rl011.local"` and `"pmd-user1@rl011.local"`.

Output:



```
Id      Name                PSJobTypeName   State           HasMoreData     Location             Command
--      ----                -------------   -----           -----------     --------             -------
9       Job9                BackgroundJob   Running         True            localhost            ...
11      Job11               BackgroundJob   Running         True            localhost            ...
9       Job9                BackgroundJob   Completed       True            localhost            ...
11      Job11               BackgroundJob   Completed       True            localhost            ...

Jobs completed, getting outputs....

----------------------------------- JobId=[9] ------------------------------------------
Start job for UPN=[pmd-user2@rl011.local].
Sending logoff resources request...
Logoff resources successfully.
Complete job for UPN=[pmd-user2@rl011.local].
----------------------------------- End --------------------------------------------------

----------------------------------- JobId=[11] ------------------------------------------
Start job for UPN=[pmd-user1@rl011.local].
Sending logoff resources request...
Logoff resources successfully.
Complete job for UPN=[pmd-user1@rl011.local].
----------------------------------- End --------------------------------------------------
```

Note that this API simply issues the log off request and does not wait for the sessions to complete logging off.

NetScaler for Load Balancing Multiple Session Remote Start Servers

December 13, 2024

Session Remote Start supports multiple servers to load balance the requests effectively. We recommend using NetScaler as a Load Balancer.

NetScaler Configuration

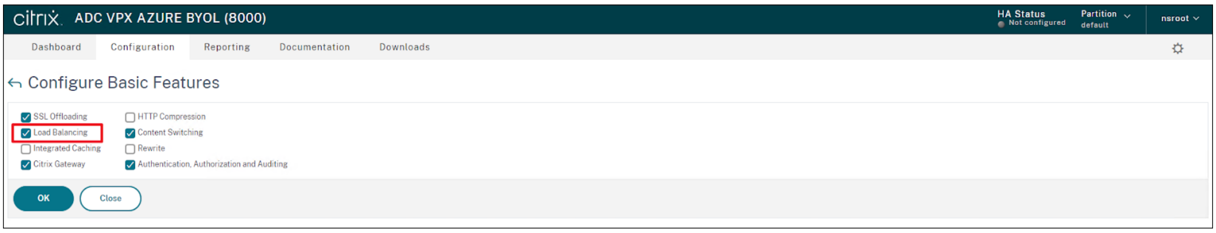
System Requirements for NetScaler as a Load Balancer

The following table lists the minimum requirements.

OS	NetScalerVPX 13.1
Processor	4 or more cores on a compatible 64-bit processor
RAM	Min 8GB
Storage	50 GB

Enable load balancing

Navigate to **System > Settings**, and in **Configure Basic Features**, select **Load Balancing**.



Configure Basic Features

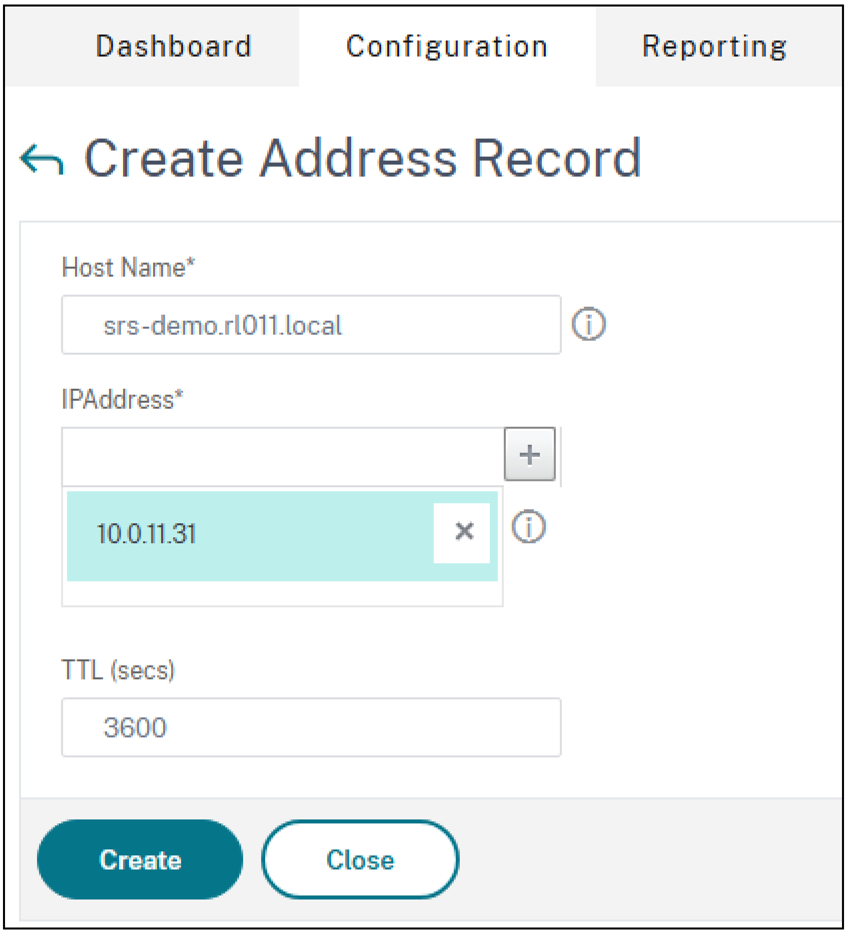
☑ SSL Offloading
☑ Load Balancing
☐ Integrated Caching
☑ Citrix Gateway
☐ HTTP Compression
☑ Content Switching
☐ Rewrite
☑ Authentication, Authorization and Auditing

Configure server objects

Create an entry for your server on the NetScaler appliance. The NetScaler appliance supports IP address based servers and domain-based servers. If you create an IP address based server, you can specify the name of the server instead of its IP address when you create a service.

1. If you want to specify the name of the server instead of its IP address, add an address record first. Otherwise, skip this step.

Navigate to **Traffic Management > DNS > Records > Address Records**, and add an address record.



Create Address Record

Host Name*

srs-demo.rl011.local

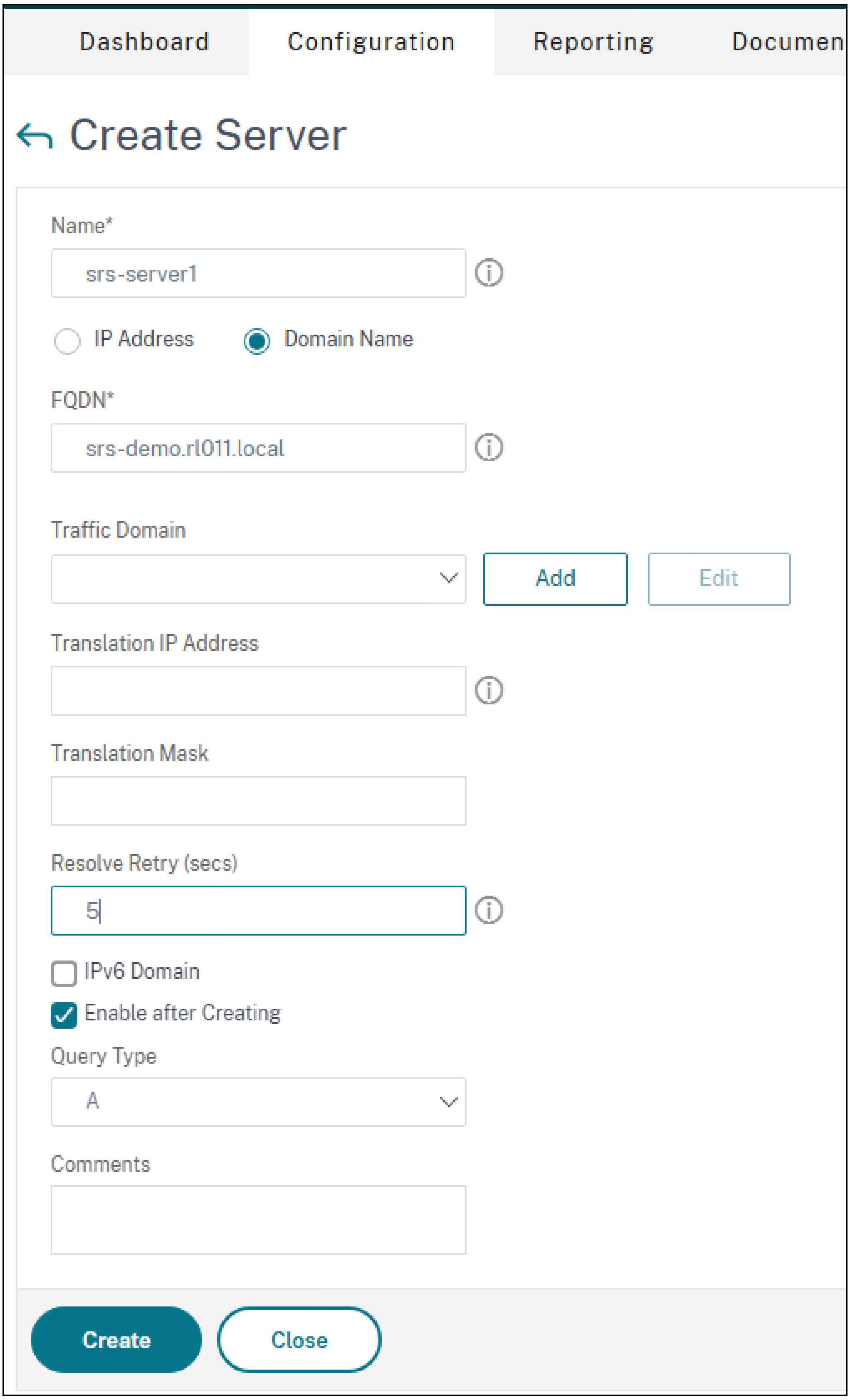
IPAddress*

10.0.11.31

TTL (secs)

3600

1. Navigate to **Traffic Management > Load Balancing > Servers**, and add a server object.



Create Server

Name*: srs-server1

○ IP Address ● Domain Name

FQDN*: srs-demo.rl011.local

Traffic Domain:

Translation IP Address:

Translation Mask:

Resolve Retry (secs): 5

☐ IPv6 Domain

☑ Enable after Creating

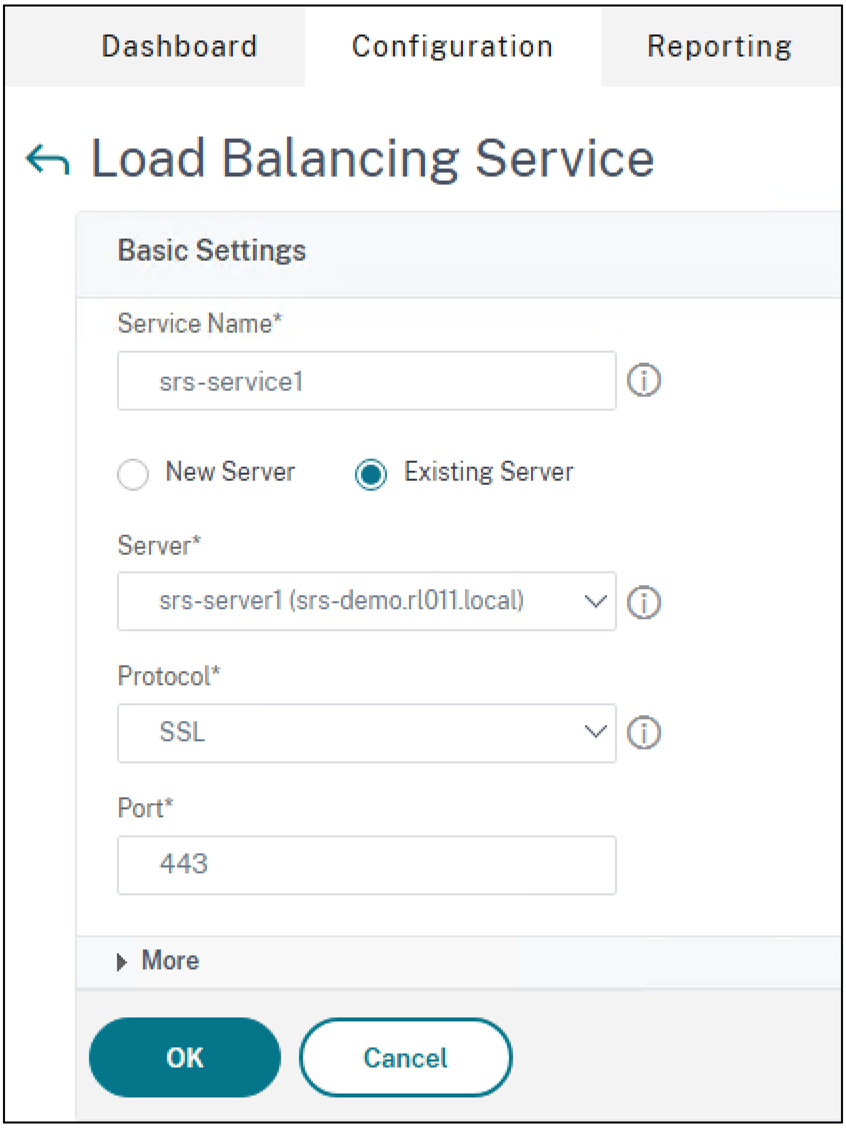
Query Type: A

Comments:

Repeat the two steps if you have multiple servers.

Configure services

1. Navigate to **Traffic Management> Load Balancing > Services**, and add a service.



Load Balancing Service

Basic Settings

Service Name*: srs-service1

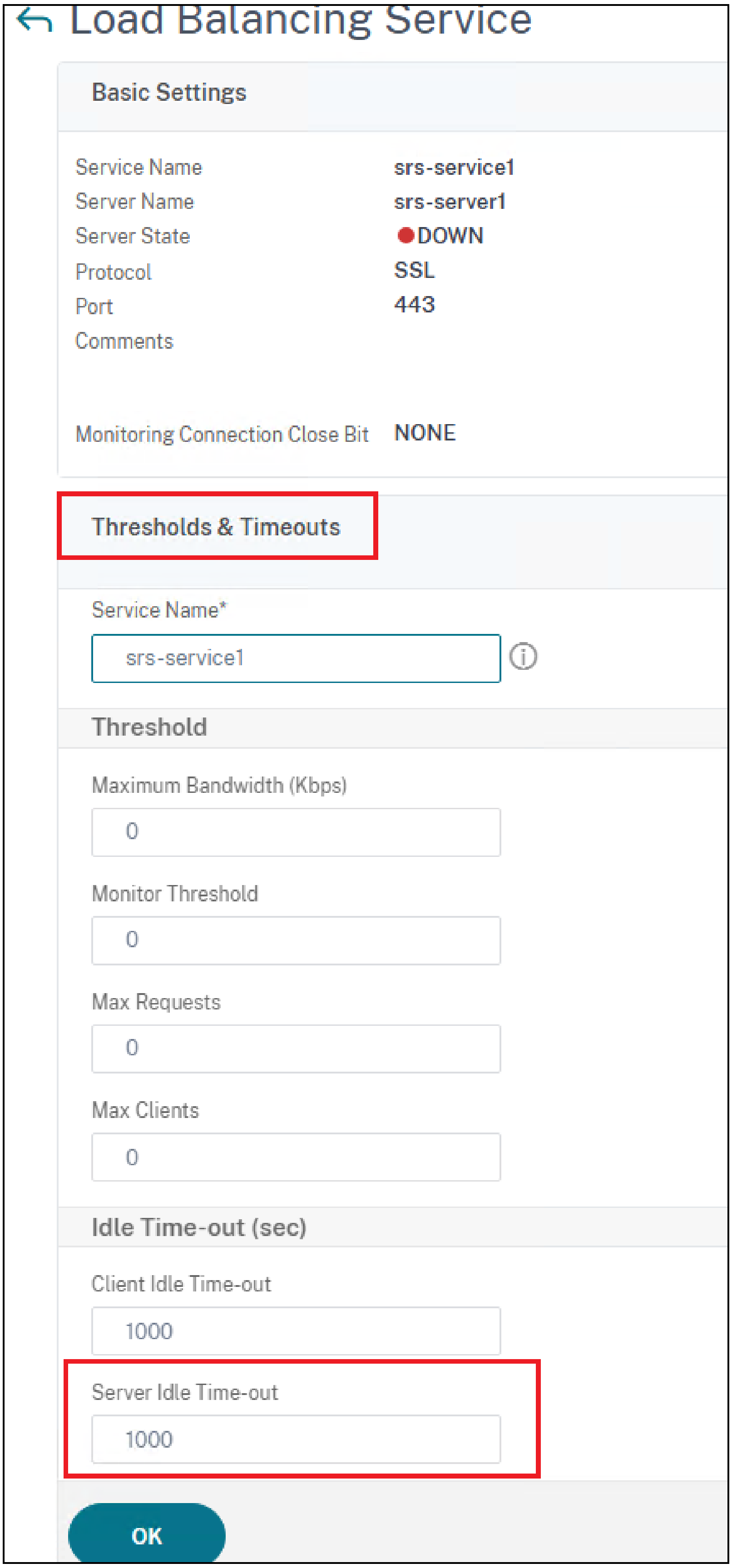
○ New Server ● Existing Server

Server*: srs-server1 (srs-demo.rl011.local)

Protocol*: SSL

Port*: 443

2. In **Thresholds & Timeouts**, modify the value of **Server Idle Time-out** according to the average launching processing seconds in your environment.



Load Balancing Service

Basic Settings

Service Name	srs-service1
Server Name	srs-server1
Server State	●DOWN
Protocol	SSL
Port	443
Comments	
Monitoring Connection Close Bit	NONE

Thresholds & Timeouts

Service Name*: srs-service1

Threshold

Maximum Bandwidth (Kbps): 0

Monitor Threshold: 0

Max Requests: 0

Max Clients: 0

Idle Time-out (sec)

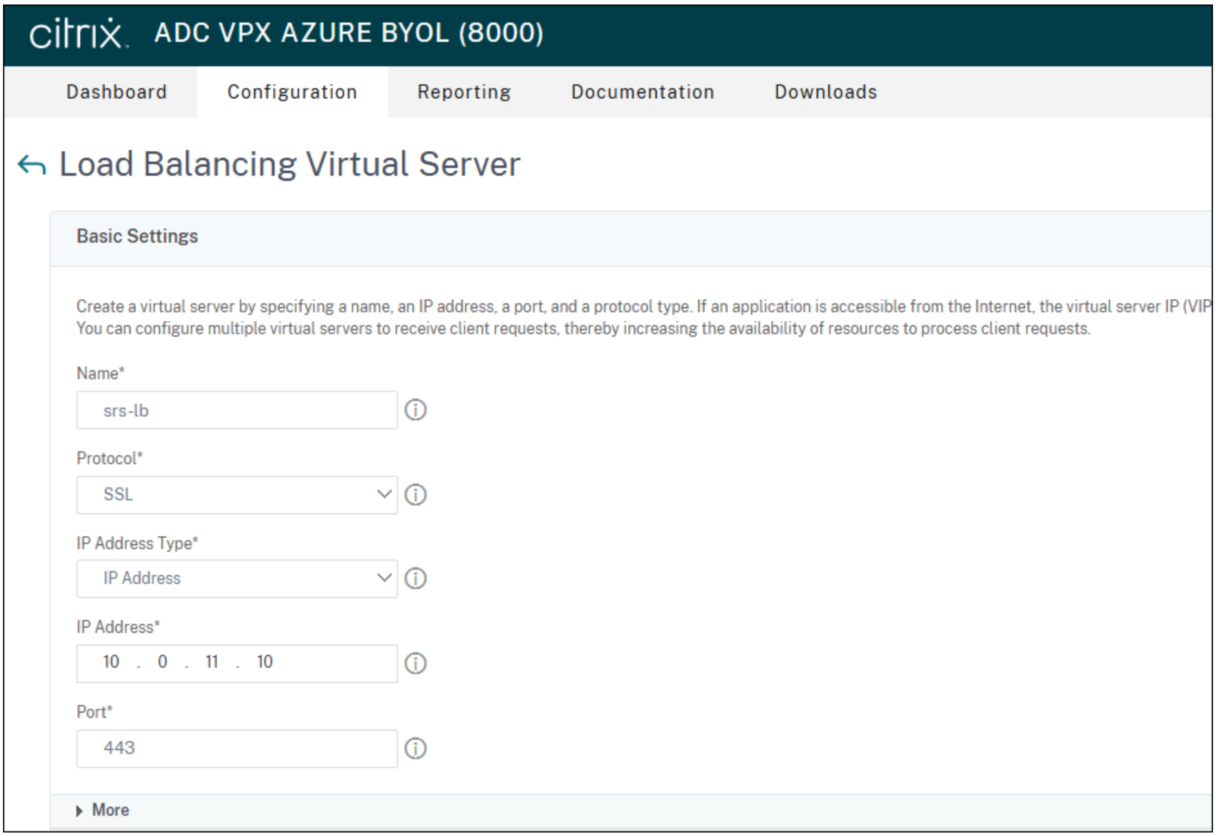
Client Idle Time-out: 1000

Server Idle Time-out: 1000

Repeat the operation if you have multiple servers.

Create a virtual server

1. Navigate to **Traffic Management > Load Balancing > Virtual Servers**, and then create a virtual server.



Load Balancing Virtual Server

Basic Settings

Create a virtual server by specifying a name, an IP address, a port, and a protocol type. If an application is accessible from the Internet, the virtual server IP (VIP
You can configure multiple virtual servers to receive client requests, thereby increasing the availability of resources to process client requests.

Name*: srs-lb

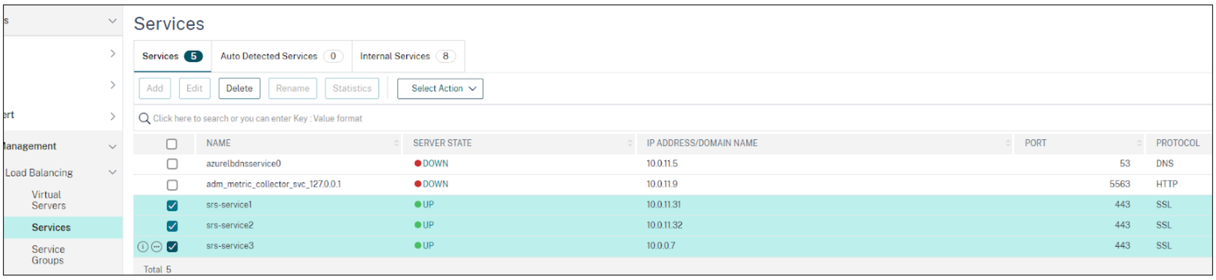
Protocol*: SSL

IP Address Type*: IP Address

IP Address*: 10 . 0 . 11 . 10

Port*: 443

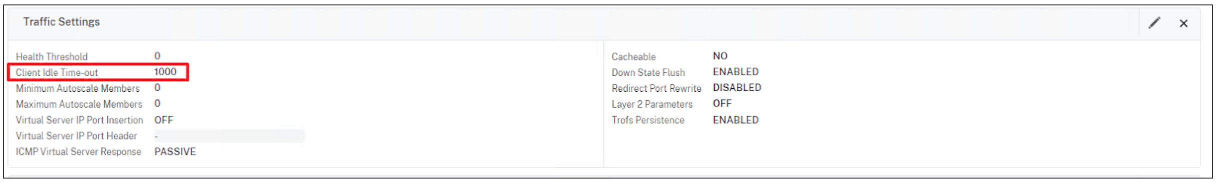
1. Bind services to the virtual server.



	NAME	SERVER STATE	IP ADDRESS/DOMAIN NAME	PORT	PROTOCOL
□	azurelbdnsservice0	● DOWN	10.0.11.5	53	DNS
□	adm_metric_collector_svc_127.0.0.1	● DOWN	10.0.11.9	5563	HTTP
☑	srs-service1	● UP	10.0.11.31	443	SSL
☑	srs-service2	● UP	10.0.11.32	443	SSL
☑	srs-service3	● UP	10.0.0.7	443	SSL

Total 5

1. In **Traffic Settings**, modify the value of **Client Idle Time-out** according to the average launching processing seconds in your environment.

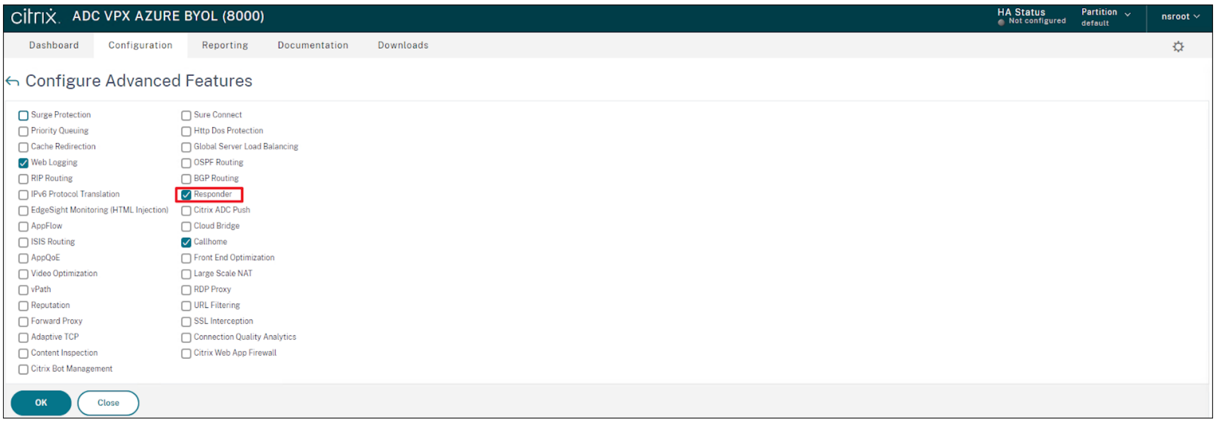


Traffic Settings

Health Threshold	0	Cacheable	NO
Client Idle Time-out	1000	Down State Flush	ENABLED
Minimum Autoscale Members	0	Redirect Port Rewrite	DISABLED
Maximum Autoscale Members	0	Layer 2 Parameters	OFF
Virtual Server IP Port Insertion	OFF	Trofs Persistence	ENABLED
Virtual Server IP Port Header	-		
ICMP Virtual Server Response	PASSIVE		

Configure a Responder Policy to drop untrusted IP addresses (Optional)

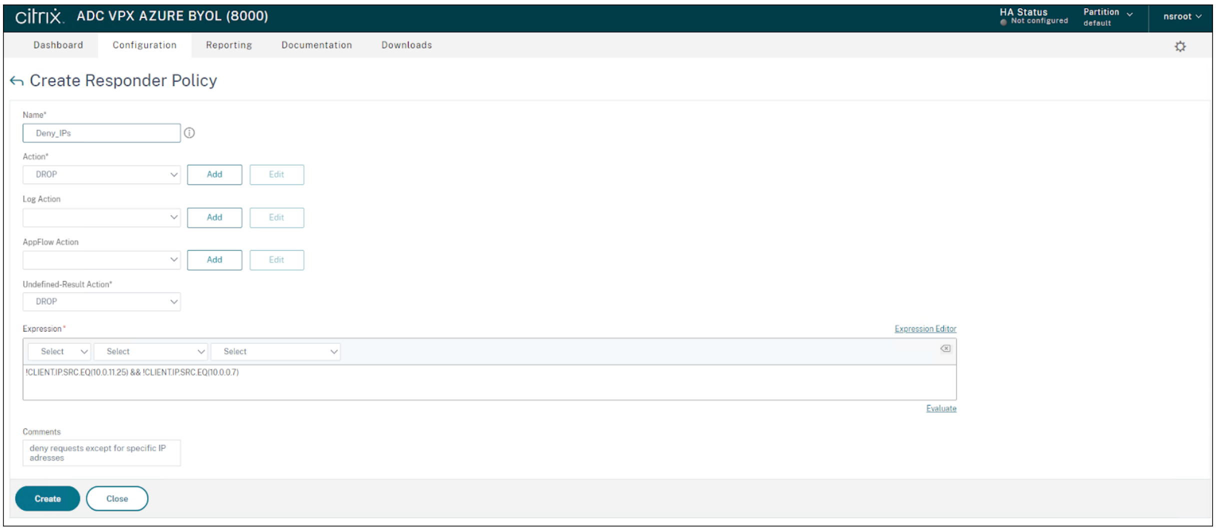
1. Enable the responder feature. Navigate to **System > Settings**, and in **Configure Advanced Features**, select **Responder**.



Configure Advanced Features

☐ Surge Protection
☐ Priority Queuing
☐ Cache Redirection
☑ Web Logging
☐ RIP Routing
☐ IPv6 Protocol Translation
☐ EdgeSight Monitoring (HTML Injection)
☐ AppFlow
☐ ISIS Routing
☐ AppQoE
☐ Video Optimization
☐ vPath
☐ Reputation
☐ Forward Proxy
☐ Adaptive TCP
☐ Content Inspection
☐ Citrix Bot Management
☐ Sure Connect
☐ Http Dos Protection
☐ Global Server Load Balancing
☐ OSPF Routing
☐ BGP Routing
☑ Responder
☐ Citrix ADC Push
☐ Cloud Bridge
☑ Callhome
☐ Front End Optimization
☐ Large Scale NAT
☐ RDP Proxy
☐ URL Filtering
☐ SSL Interception
☐ Connection Quality Analytics
☐ Citrix Web App Firewall

1. Configure a responder policy. Navigate to **AppExpert > Responder > Policies**, and add a policy.



Create Responder Policy

Name*: Deny_IPs

Action*: DROP

Log Action:

AppFlow Action:

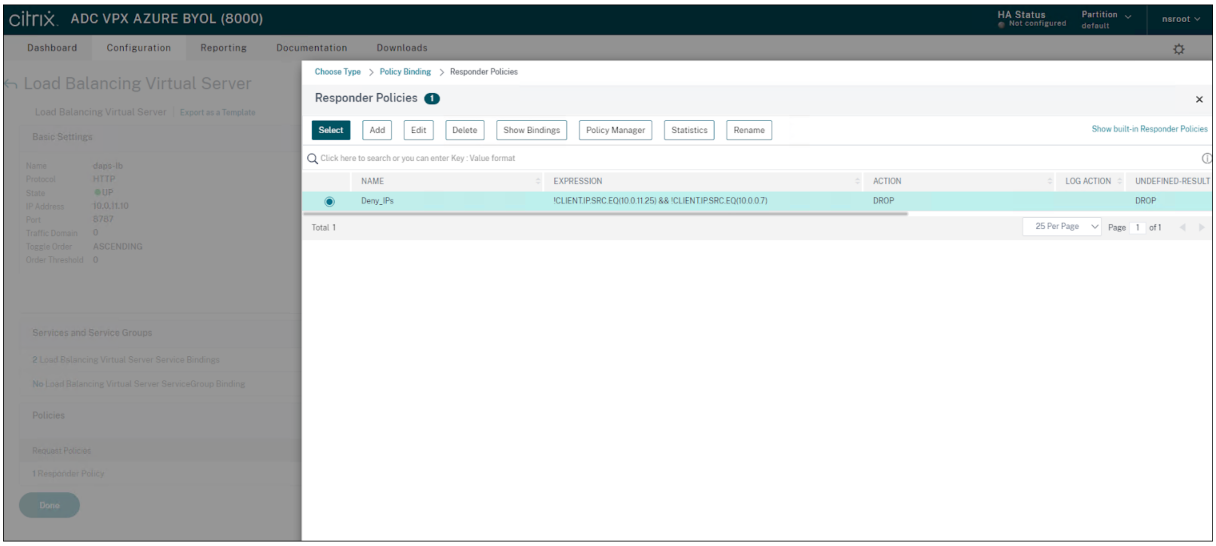
Undefined-Result Action*: DROP

Expression*: !CLIENT.IP.SRC.EQ(10.0.11.25) && !CLIENT.IP.SRC.EQ(10.0.0.7)

Comments: deny requests except for specific IP adresses

In this example, the policy drops any request except for the ones from the specific IP addresses - 10.0.11.25/10.0.0.7.

Bind policy to the virtual server. Navigate to **Traffic Management > Load Balancing > Virtual Servers**. On the **Load Balancing Virtual Servers** page, select the virtual server to which you want to bind the responder policy, and then click **Open**.



Load Balancing Virtual Server

Load Balancing Virtual Server | Export as a Template

Basic Settings

Name	daps-lb
Protocol	HTTP
State	UP
IP Address	10.0.11.10
Port	8787
Traffic Domain	0
Toggle Order	ASCENDING
Order Threshold	0

Services and Service Groups

2 Load Balancing Virtual Server Service Bindings

No Load Balancing Virtual Server ServiceGroup Binding

Policies

Request Policies

1 Responder Policy

Responder Policies 1

	NAME	EXPRESSION	ACTION	LOG ACTION	UNDEFINED-RESULT
●	Deny_IPs	!CLIENT.IP.SRC.EQ(10.0.11.25) && !CLIENT.IP.SRC.EQ(10.0.0.7)	DROP		DROP

Total 1

StoreFront Configuration

Gateway Configuration

1. Add each Session Remote Start as a gateway following 'Add Session Remote Start as a Gateway' section.
2. Apply each gateway to the Session Remote Start store following the 'Configure Remote Access Settings'section.

StoreFront Plugin Configuration

Add each Session Remote Start URL to 'srs_server_urls'following 'Configure Session Remote Start plugin'section.

FAQ

December 11, 2024

Response 404 - UPNNotFound

It may not really be caused by UPNNotFound, but most caused by StoreFront authentication for various reasons:

1. Communication error between Session Remote Start and StoreFront

   a) Open Web.config, double confirm the 'StoreFrontServer'option. A recommended practice is to set 'StoreFrontServer'by copy from 'Receiver from Web Sites'in StoreFront UI. Please note that the StoreFront store name is case-sensitive.
   b) Try to open 'StoreFrontServer'by browser, check if there is a connection or certificate error. (Do not need to login, just check if the web page can be visited normally.)
   c) Open CDF trace tool or enable Session Remote Start log file, check if there is any error detail.

2. StoreFront issue
   Open Event Viewer -> Applications and Services Logs -> Citrix Delivery Services to check StoreFront log
3. FAS issue
   For step #2, the error may be related to FAS, please refer to the FAS section of the checklist above.

Request Timeout

- Session Remote Start has a 'RequestTimeoutSeconds'option in Web.config. When request duration reaches the timeout, Session Remote Start will respond with status code 408 and body content.
- Session Remote Start will never terminate http connection without response. Please check if there is any timeout related setting in the caller.
- For the 'LaunchResource'API, there is an optional parameter 'WaitForLogonNotification'recognized as true by default. For the VDAs really take a long time for launching, 'WaitForLogonNotification'can be set to false. API will respond immediately and execute the launching process in the backend.

Known issues

January 15, 2025

The **Launch All Desktops by Tags** feature has a limitation when configured with any of the following two settings:

- When a tag is applied to a **Static Delivery Group**.
- If the desktops within a delivery group are assigned to an Active Directory (AD) group instead of individual users.

The feature will not be able to retrieve and launch those desktops.

Optional Configurations

January 15, 2025

1. Change Log File location and Permissions

If the Log File location is changed, make sure that the Session Remote Start service has the necessary permissions to modify the log file.

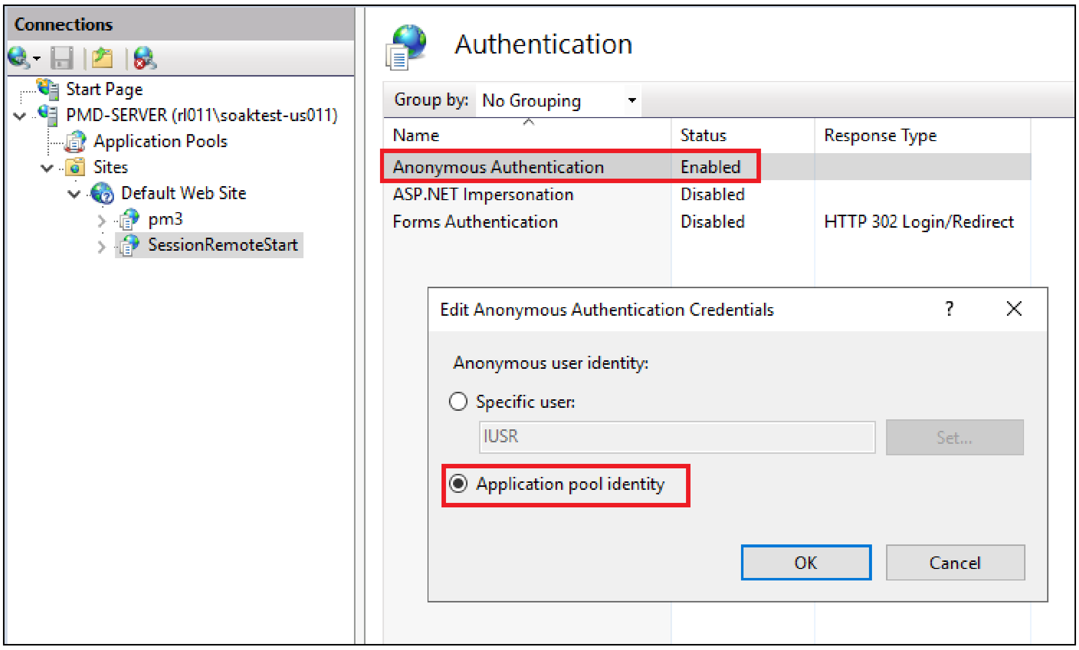
Log file permissions

1. Set an anonymous user identity to Application Pool Identity.

    a) Open **IIS Manager > Sites > Default Web Site > SessionRemoteStart** and then open **Authentication** under **SessionRemoteStart Home** page.

    a) Right-click **Anonymous Authentication** and click **Enable**.

    b) Right-click **Anonymous Authentication** and select **Edit > Select Application pool identity**.



Name	Status	Response Type
Anonymous Authentication	Enabled	
ASP.NET Impersonation	Disabled	
Forms Authentication	Disabled	HTTP 302 Login/Redirect

Edit Anonymous Authentication Credentials

Anonymous user identity:

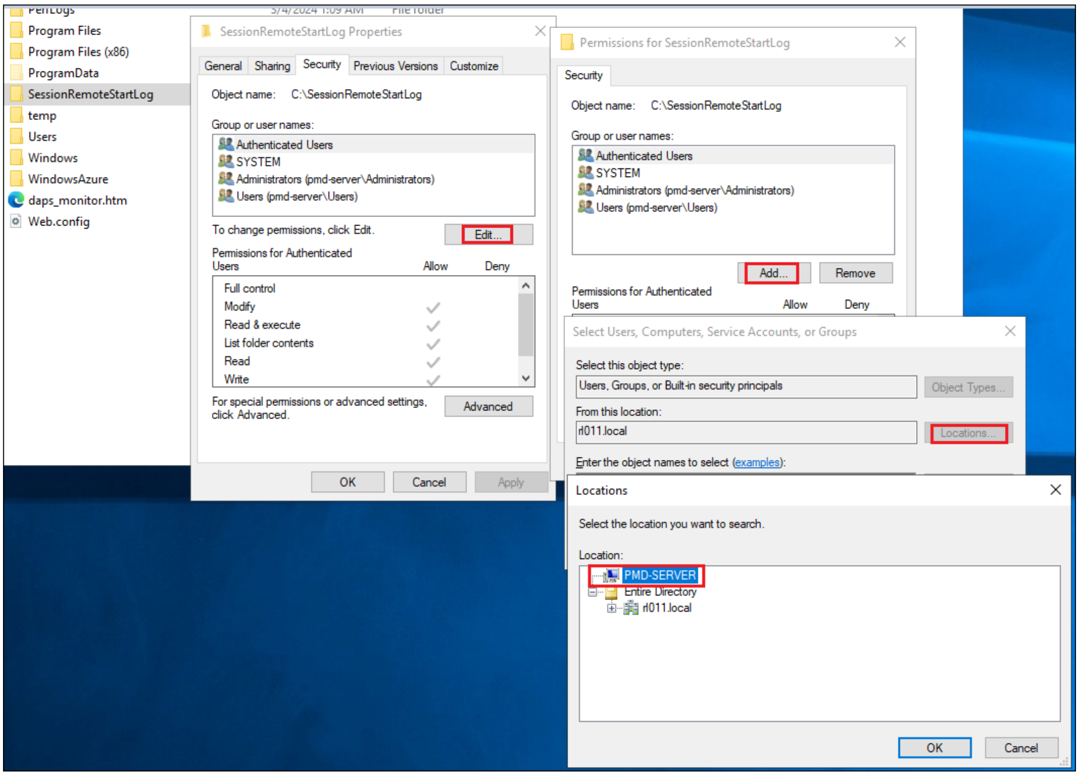
○ Specific user:

IUSR

● Application pool identity

2. Now you can create a folder at your preferred location, and grant permissions to log to the new folder.

a) For example, after the folder creation under C:\SessionRemoteStartLog, right-click the folder and select **Properties**. In the **Security** tab, click **Edit** under **Group or user names** and then select **Add** to change the location to a local computer.



SessionRemoteStartLog Properties

Object name: C:\SessionRemoteStartLog

Group or user names:
Authenticated Users
SYSTEM
Administrators (pmd-server\Administrators)
Users (pmd-server\Users)

Permissions for SessionRemoteStartLog

Object name: C:\SessionRemoteStartLog

Select Users, Computers, Service Accounts, or Groups

Select this object type: Users, Groups, or Built-in security principals

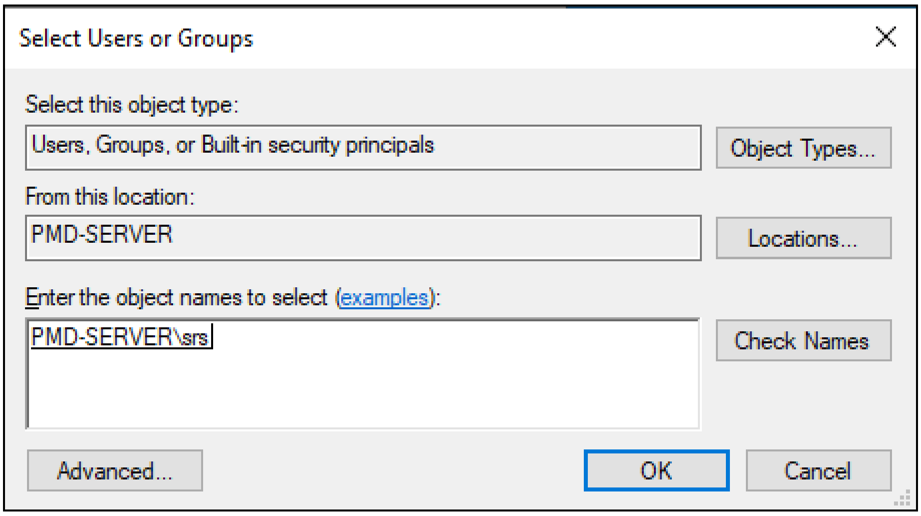
From this location: rl011.local

Locations

Select the location you want to search.

Location: PMD-SERVER

b) Input the Session Remote Start user created in the previous section. (If the default identity is used, input "IIS AppPool\SrsAppPool"instead).



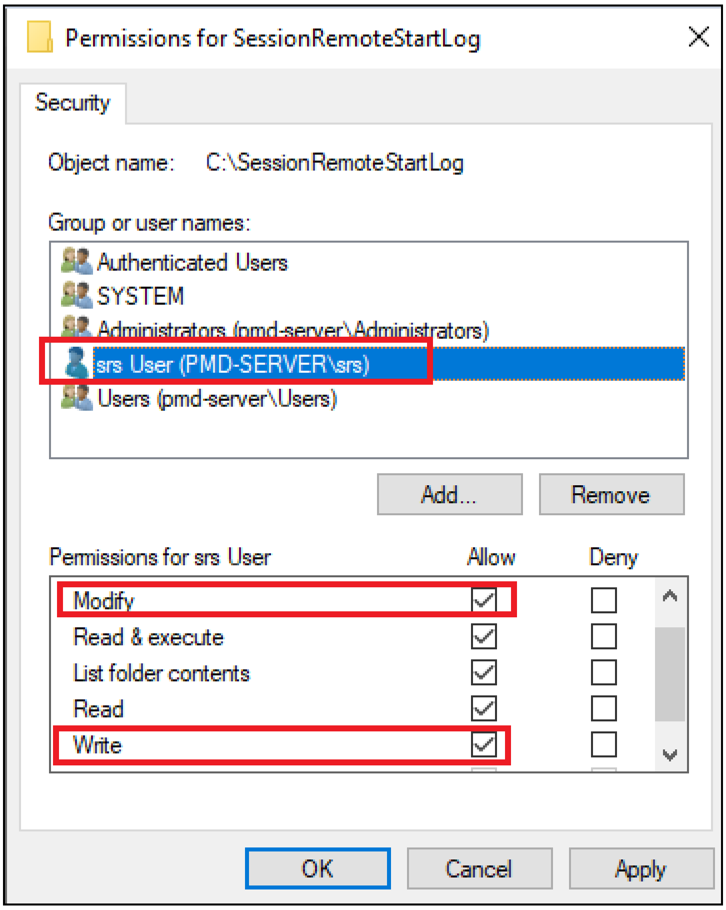
Select Users or Groups

Select this object type: Users, Groups, or Built-in security principals

From this location: PMD-SERVER

Enter the object names to select (examples): PMD-SERVER\srs

c) Grant **Modify** and **Write** permissions. (If the default identity is used, grant access to **SrsAppPool**)



Permissions for SessionRemoteStartLog

Security

Object name: C:\SessionRemoteStartLog

Group or user names:

- Authenticated Users
- SYSTEM
- Administrators (pmd-server\Administrators)
- srs User (PMD-SERVER\srs)
- Users (pmd-server\Users)

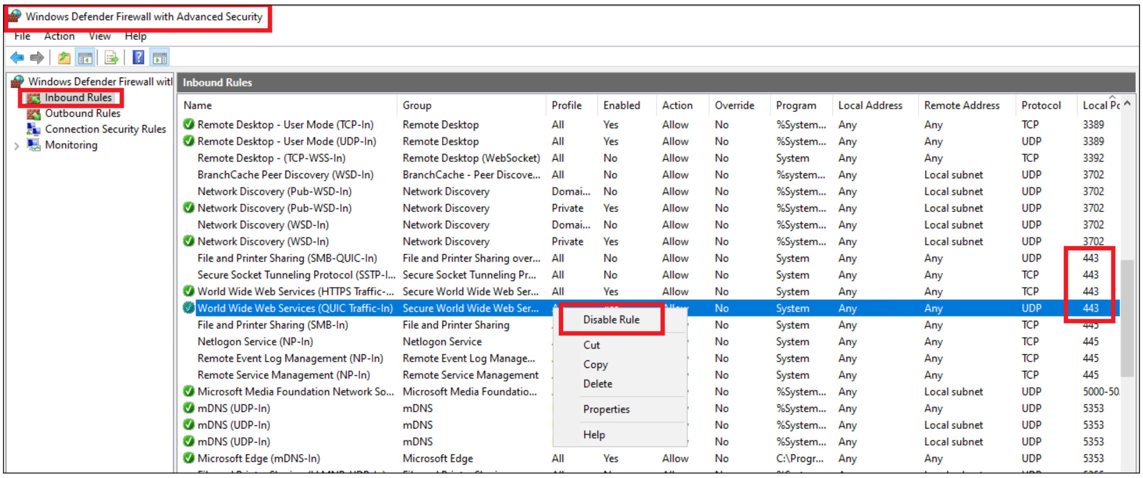
Permissions for srs User	Allow	Deny
Modify	☑	□
Read & execute	☑	□
List folder contents	☑	□
Read	☑	□
Write	☑	□

2. Configure Inbound Firewall Rules

Specifying IP addresses and host names of the trusted services and StoreFront ensures that only these sources can communicate with Session Remote Start and helps to prevent DoS or other opportunistic attacks against the Session Remote Start server.

After creating the https binding on port 443, customers can configure inbound firewall rules by 'Windows Defender Firewall with Advanced Security'UI to allow inbound TCP traffic.

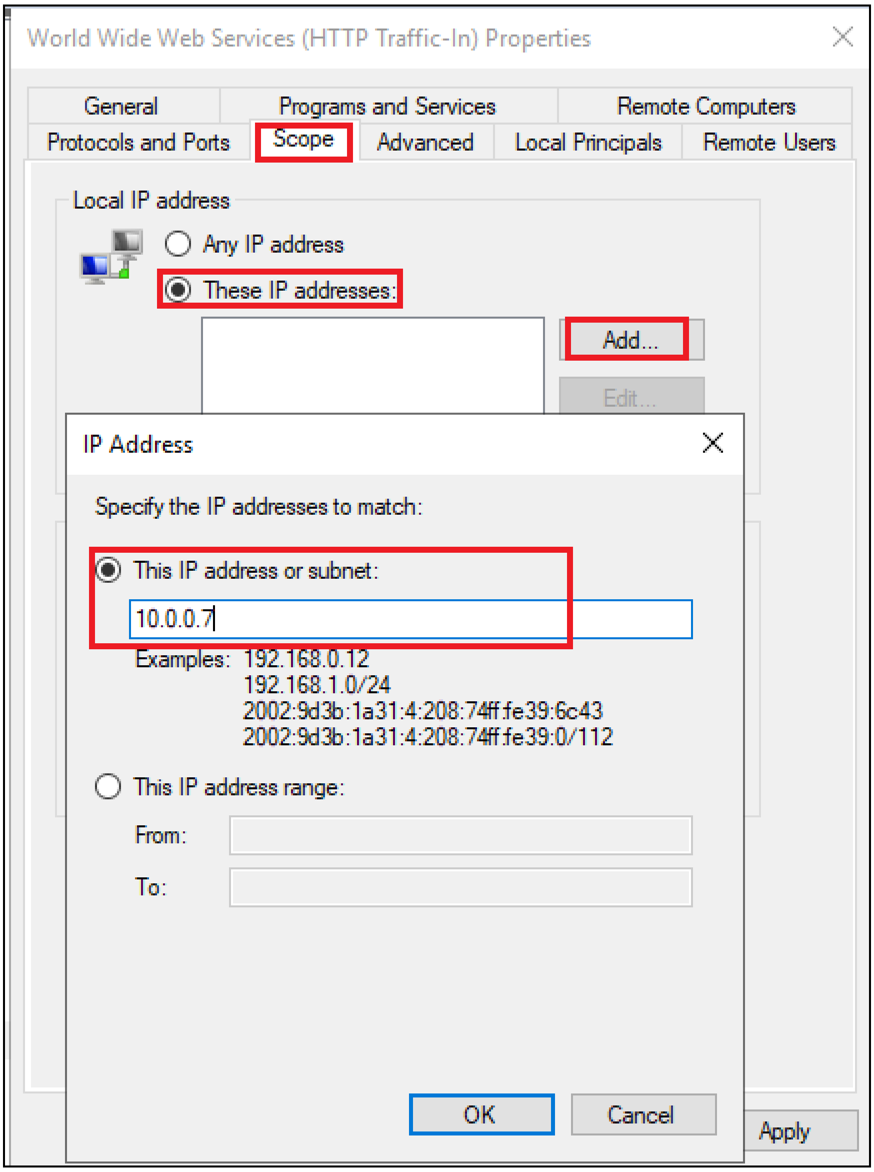
1. Disable all 443 inbound rules except **World Wide Web Service (HTTPS Traffic-In)**.



Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Pc
✓ Remote Desktop - User Mode (TCP-In)	Remote Desktop	All	Yes	Allow	No	%System...	Any	Any	TCP	3389
✓ Remote Desktop - User Mode (UDP-In)	Remote Desktop	All	Yes	Allow	No	%System...	Any	Any	UDP	3389
Remote Desktop - (TCP-WSS-In)	Remote Desktop (WebSocket)	All	No	Allow	No	System	Any	Any	TCP	3392
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove...	All	No	Allow	No	%system...	Any	Local subnet	UDP	3702
Network Discovery (Pub-WSD-In)	Network Discovery	Domai...	No	Allow	No	%System...	Any	Local subnet	UDP	3702
✓ Network Discovery (Pub-WSD-In)	Network Discovery	Private	Yes	Allow	No	%System...	Any	Local subnet	UDP	3702
Network Discovery (WSD-In)	Network Discovery	Domai...	No	Allow	No	%System...	Any	Local subnet	UDP	3702
✓ Network Discovery (WSD-In)	Network Discovery	Private	Yes	Allow	No	%System...	Any	Local subnet	UDP	3702
File and Printer Sharing (SMB-QUIC-In)	File and Printer Sharing over...	All	No	Allow	No	System	Any	Any	UDP	443
Secure Socket Tunneling Protocol (SSTP-I...	Secure Socket Tunneling Pr...	All	No	Allow	No	System	Any	Any	TCP	443
✓ World Wide Web Services (HTTPS Traffic-...	Secure World Wide Web Ser...	All	Yes	Allow	No	System	Any	Any	TCP	443
✓ World Wide Web Services (QUIC Traffic-In)	Secure World Wide Web Ser...				No	System	Any	Any	UDP	443
File and Printer Sharing (SMB-In)	File and Printer Sharing				No	System	Any	Any	TCP	445
Netlogon Service (NP-In)	Netlogon Service				No	System	Any	Any	TCP	445
Remote Event Log Management (NP-In)	Remote Event Log Manage...				No	System	Any	Any	TCP	445
Remote Service Management (NP-In)	Remote Service Management				No	System	Any	Any	TCP	445
✓ Microsoft Media Foundation Network So...	Microsoft Media Foundatio...				No	%System...	Any	Local subnet	UDP	5000-50
✓ mDNS (UDP-In)	mDNS				No	%System...	Any	Any	UDP	5353
✓ mDNS (UDP-In)	mDNS				No	%System...	Any	Local subnet	UDP	5353
✓ mDNS (UDP-In)	mDNS				No	%System...	Any	Local subnet	UDP	5353
✓ Microsoft Edge (mDNS-In)	Microsoft Edge	All	Yes	Allow	No	C:\Progr...	Any	Any	UDP	5353

> **Note:**
>
> Remember to check if there are any enabled rules allowing all (all the limitations set to any) inbound traffic.

1. Double click 'World Wide Web Service (HTTPS Traffic-In)', open the 'Properties'configuration, switch to 'Scope'tab.
2. Add local IP address limitation. This is the local endpoint(s) (Network Interface) for 3rd-party Auth Service and StoreFront.



○ Any IP address

● These IP addresses:

Specify the IP addresses to match:

● This IP address or subnet:

10.0.0.7

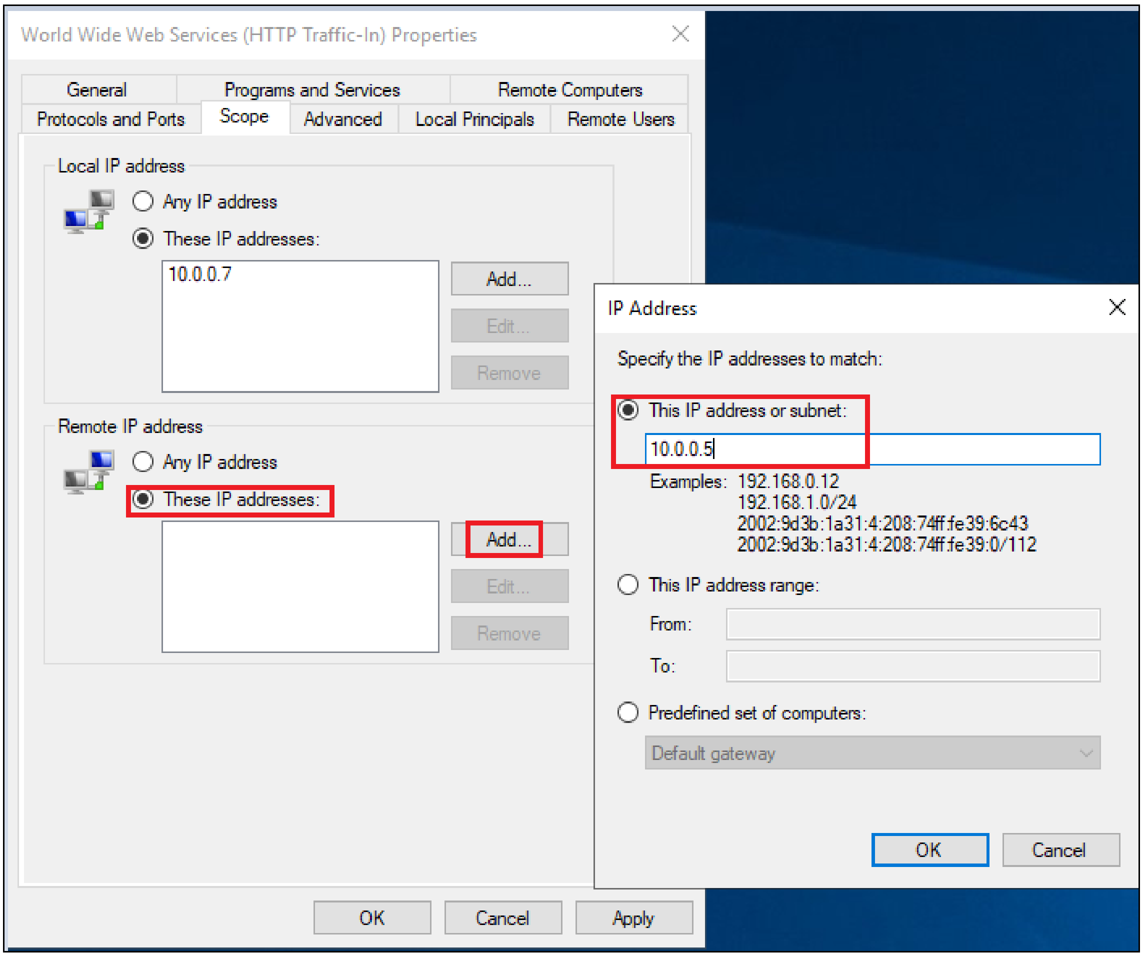
Examples: 192.168.0.12
192.168.1.0/24
2002:9d3b:1a31:4:208:74ff:fe39:6c43
2002:9d3b:1a31:4:208:74ff:fe39:0/112

○ This IP address range:

From:

To:

3. Add remote IP address limitation. Add IP addresses of 3rd-party Auth Service and StoreFront.



Local IP address

○ Any IP address

● These IP addresses:

10.0.0.7

Remote IP address

○ Any IP address

● These IP addresses:

Specify the IP addresses to match:

● This IP address or subnet:

10.0.0.5

Examples: 192.168.0.12
192.168.1.0/24
2002:9d3b:1a31:4:208:74ff:fe39:6c43
2002:9d3b:1a31:4:208:74ff:fe39:0/112

○ This IP address range:

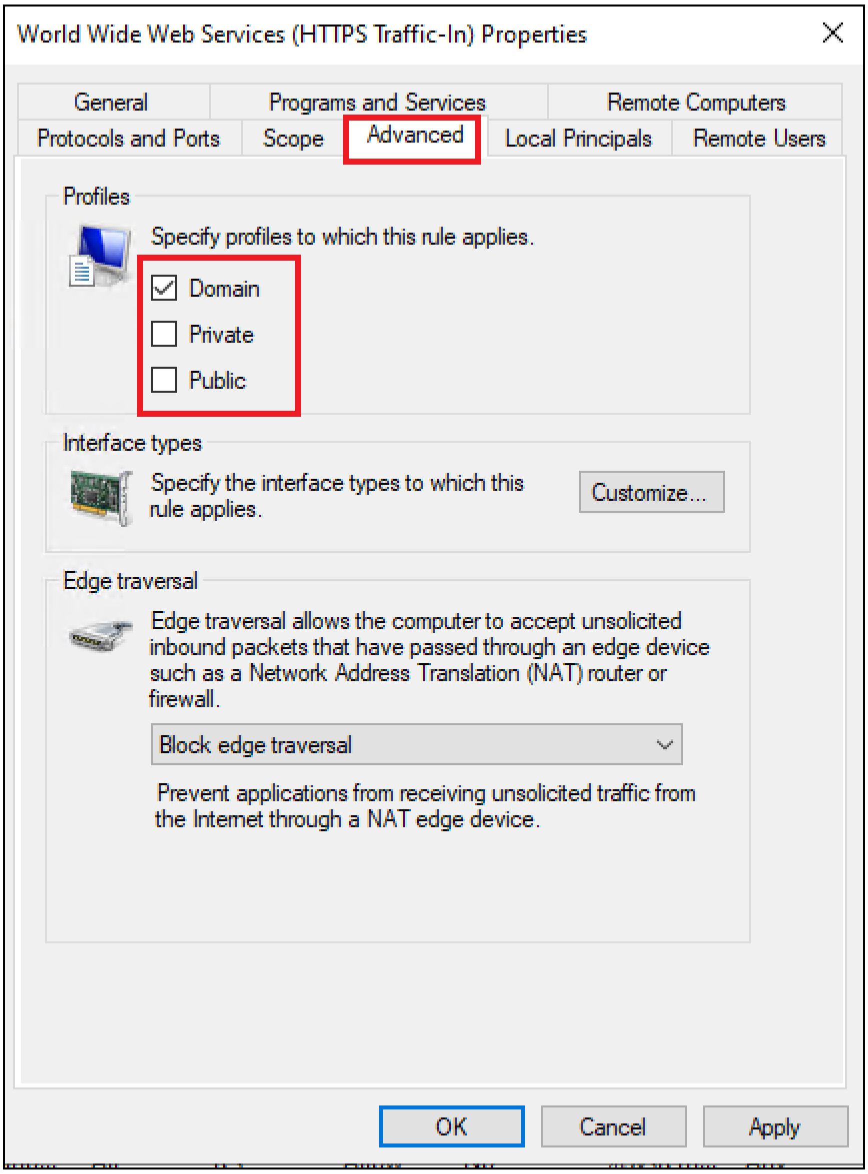
From:

To:

○ Predefined set of computers:

Default gateway

4. Switch to the **Advanced** tab and apply to related profile(s).



World Wide Web Services (HTTPS Traffic-In) Properties

Profiles

Specify profiles to which this rule applies.

☑ Domain

☐ Private

☐ Public

Interface types

Specify the interface types to which this rule applies.

Edge traversal

Edge traversal allows the computer to accept unsolicited inbound packets that have passed through an edge device such as a Network Address Translation (NAT) router or firewall.

Block edge traversal

Prevent applications from receiving unsolicited traffic from the Internet through a NAT edge device.

Third party firewall products will require configuring separately.

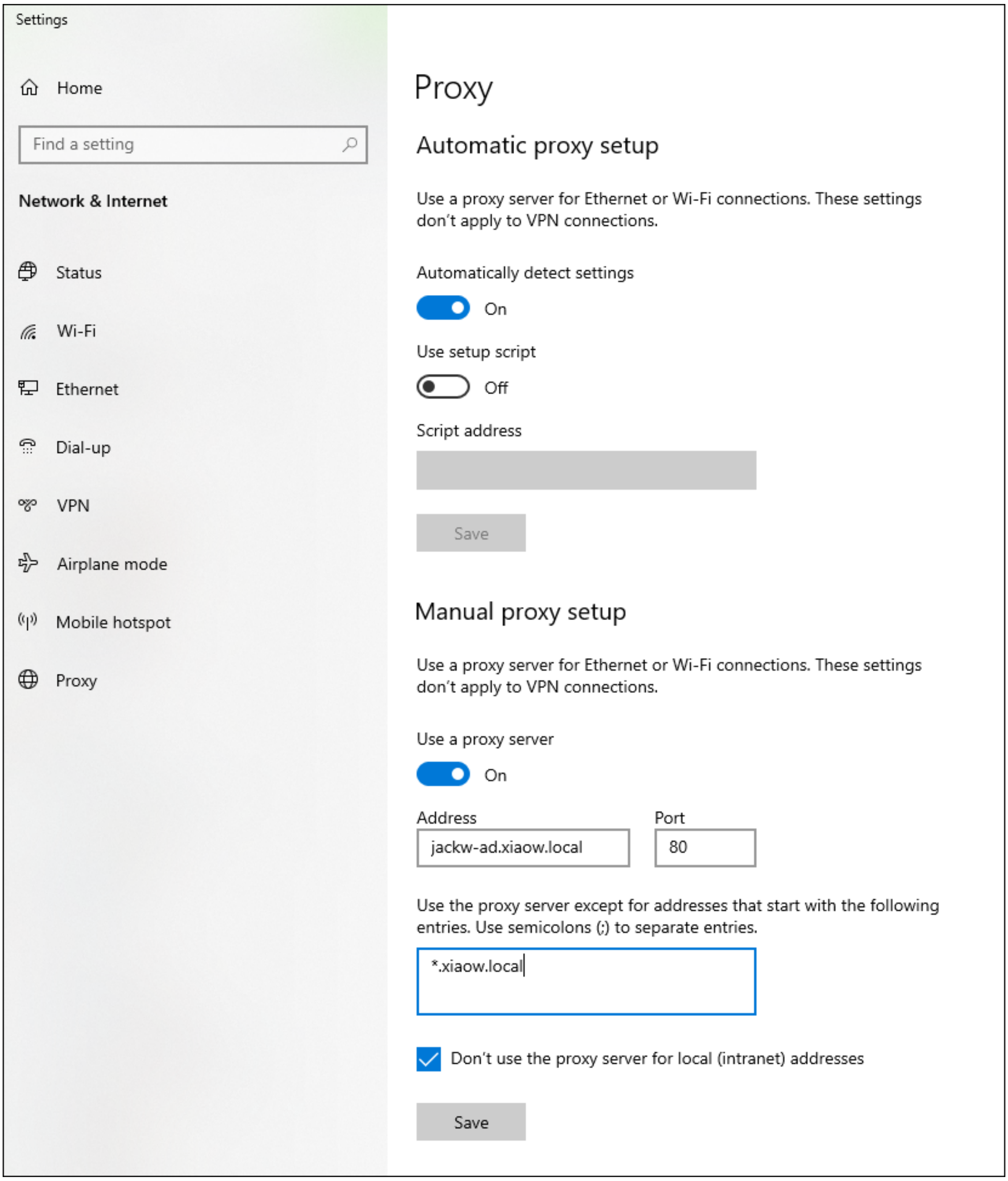
3. App Protection

If App Protection is enabled for a delivery group, the customization described in this Citrix documentation must be applied to the Session Remote Start store:

4. HTTP Proxy Configuration

Session Remote Start supports only unauthenticated HTTP proxies.

1. Configure the WinINet HTTP proxy. e.g.



Proxy

Automatic proxy setup

Use a proxy server for Ethernet or Wi-Fi connections. These settings don't apply to VPN connections.

Automatically detect settings

On

Use setup script

Off

Script address

Save

Manual proxy setup

Use a proxy server for Ethernet or Wi-Fi connections. These settings don't apply to VPN connections.

Use a proxy server

On

Address

jackw-ad.xiaow.local

Port

80

Use the proxy server except for addresses that start with the following entries. Use semicolons (;) to separate entries.

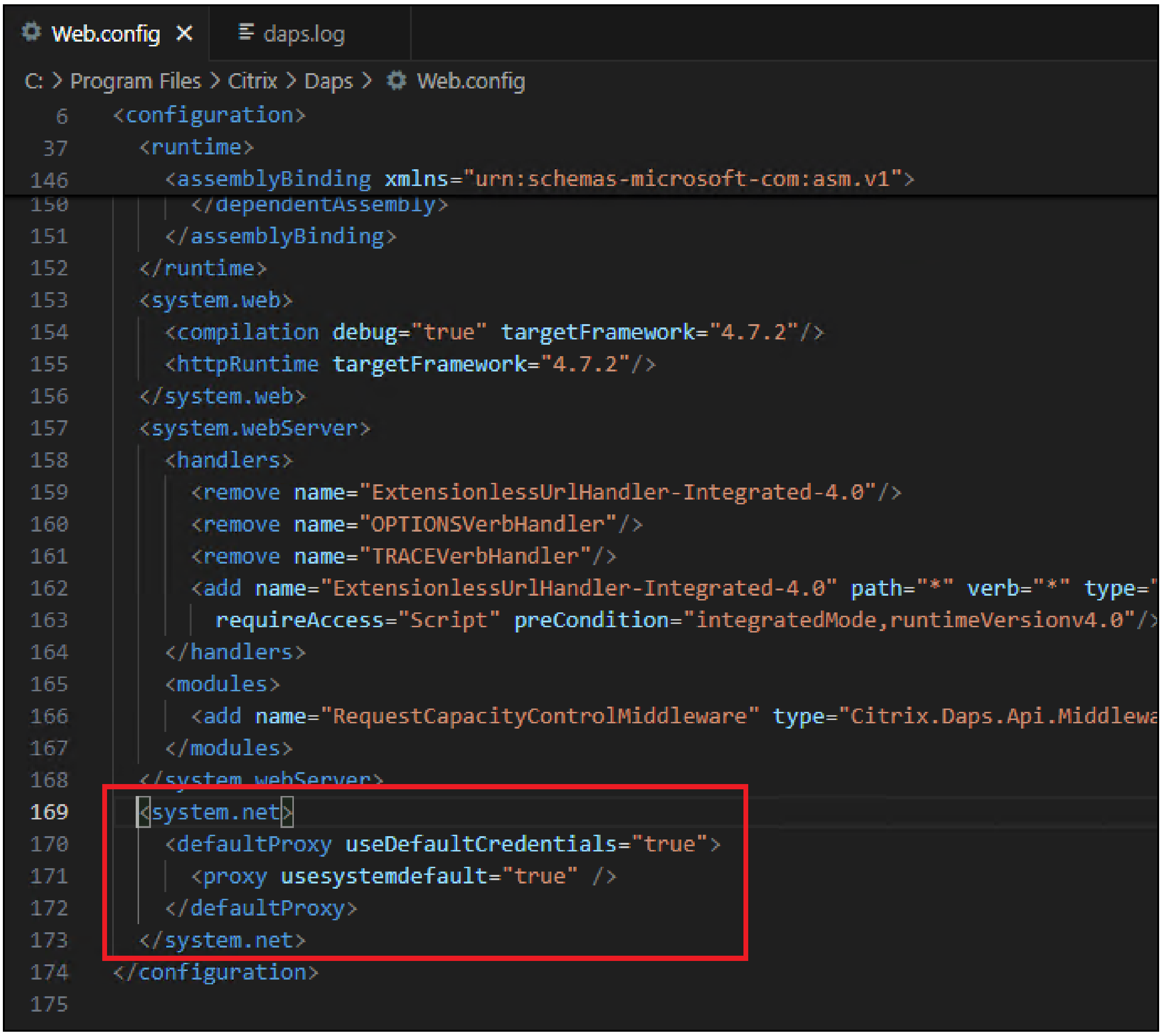
*.xiaow.local

☑ Don't use the proxy server for local (intranet) addresses

Save

2. Append the following code to `web.config`.

```
<system.net>
<defaultProxy useDefaultCredentials="true">
<proxy usesystemdefault="true"/>
</defaultProxy>
</system.net>
```

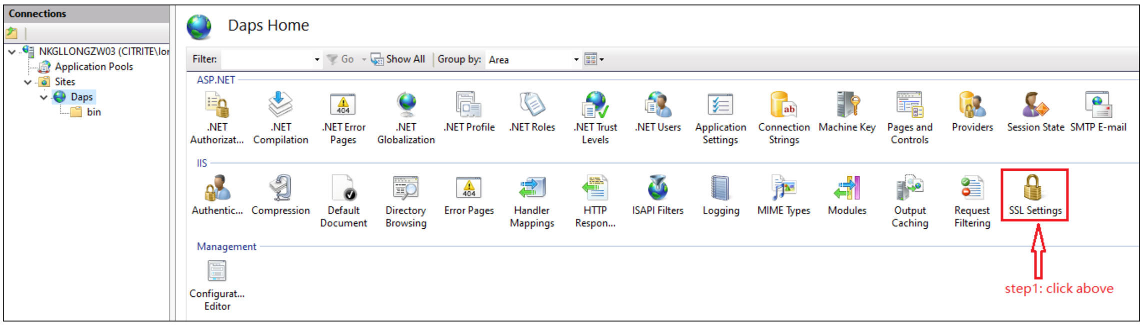


```
<configuration>
  <runtime>
    <assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">
      </dependentAssembly>
    </assemblyBinding>
  </runtime>
  <system.web>
    <compilation debug="true" targetFramework="4.7.2"/>
    <httpRuntime targetFramework="4.7.2"/>
  </system.web>
  <system.webServer>
    <handlers>
      <remove name="ExtensionlessUrlHandler-Integrated-4.0"/>
      <remove name="OPTIONSVerbHandler"/>
      <remove name="TRACEVerbHandler"/>
      <add name="ExtensionlessUrlHandler-Integrated-4.0" path="*" verb="*" type="
        requireAccess="Script" preCondition="integratedMode,runtimeVersionv4.0"/>
    </handlers>
    <modules>
      <add name="RequestCapacityControlMiddleware" type="Citrix.Daps.Api.Middlewa
    </modules>
  </system.webServer>
  <system.net>
    <defaultProxy useDefaultCredentials="true">
      <proxy usesystemdefault="true" />
    </defaultProxy>
  </system.net>
</configuration>
```

5. mTLS configuration

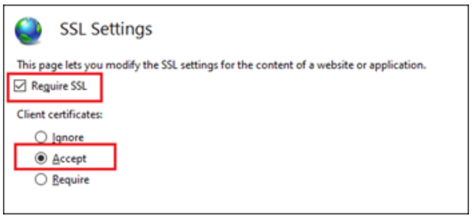
The Session Remote Start API does not require end-user authentication, unlike StoreFront. Therefore, it is crucial to ensure that only trusted services can communicate with the Session Remote Start Service. One method to achieve this is by enforcing mutual TLS (mTLS) authentication between the Session Remote Start Service and other trusted services that need access.

1. In IIS Manager, select the Session Remote Start Site, and open **SSL Settings**.



step1: click above

2. On the **SSL Settings** page, select the **Require SSL** and **Accept** check boxes and click **Apply**.



This page lets you modify the SSL settings for the content of a website or application.

☑ Require SSL

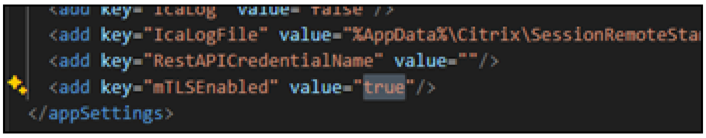
Client certificates:

○ Ignore

● Accept

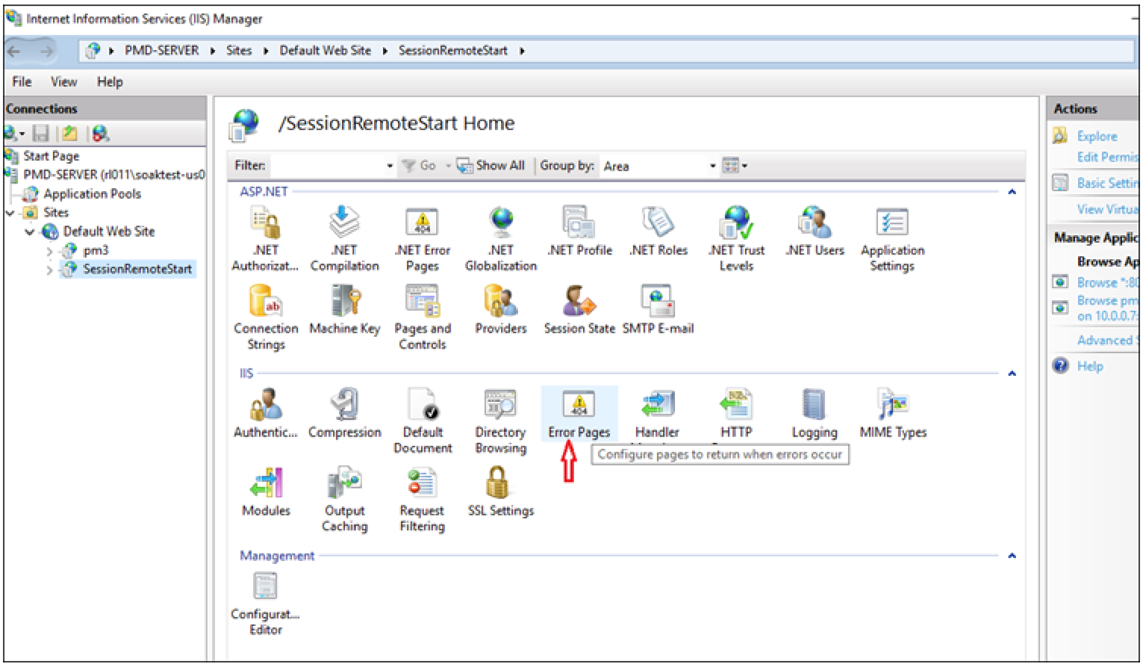
○ Require

3. Edit the Web.config and change **mTLSEnabled** to `true`.

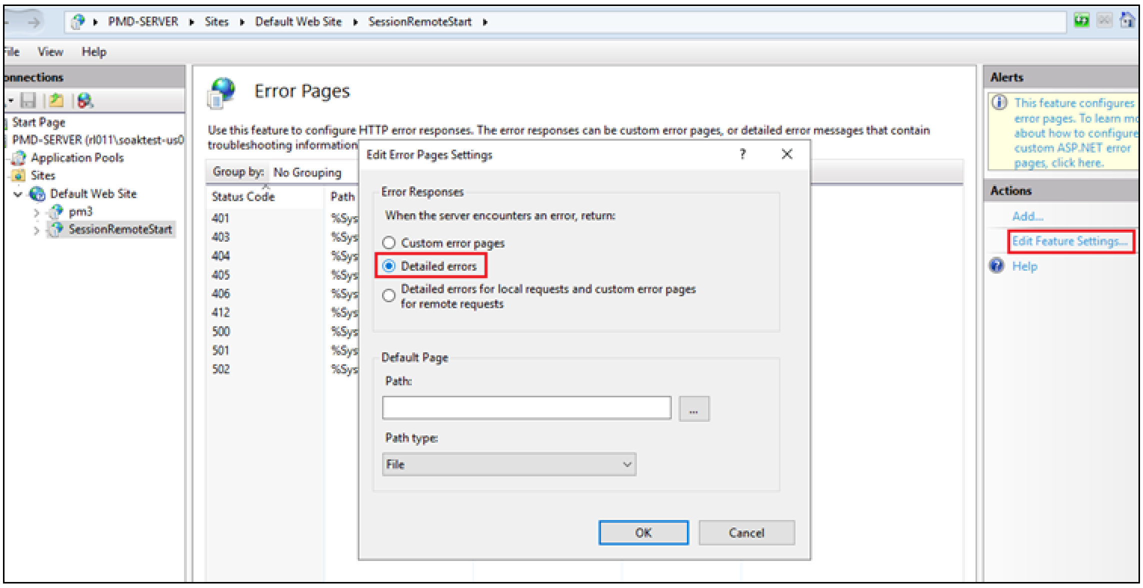


```
    <add key="IcaLog" value="false" />
    <add key="IcaLogFile" value="%AppData%\Citrix\SessionRemoteSta
    <add key="RestAPICredentialName" value=""/>
    <add key="mTLSEnabled" value="true"/>
  </appSettings>
```

4. To ensure that the responses return as expected, set the error response to **Detailed errors**.



Configure pages to return when errors occur


PMD-SERVER ▸ Sites ▸ Default Web Site ▸ SessionRemoteStart ▸
ile View Help
onnections
Start Page
PMD-SERVER (rl011\soaktest-us0
Application Pools
Sites
Default Web Site
pm3
SessionRemoteStart
Alerts
This feature configures error pages. To learn m about how to configure custom ASP.NET error pages, click here.
Actions
Add...
Edit Feature Settings...
Help
Group by: No Grouping
OK
Cancel
?
✕

Error Pages

Use this feature to configure HTTP error responses. The error responses can be custom error pages, or detailed error messages that contain troubleshooting information

Status Code	Path
401	%Sys
403	%Sys
404	%Sys
405	%Sys
406	%Sys
412	%Sys
500	%Sys
501	%Sys
502	%Sys

Edit Error Pages Settings

Error Responses

When the server encounters an error, return:

○ Custom error pages

● Detailed errors

○ Detailed errors for local requests and custom error pages for remote requests

Default Page

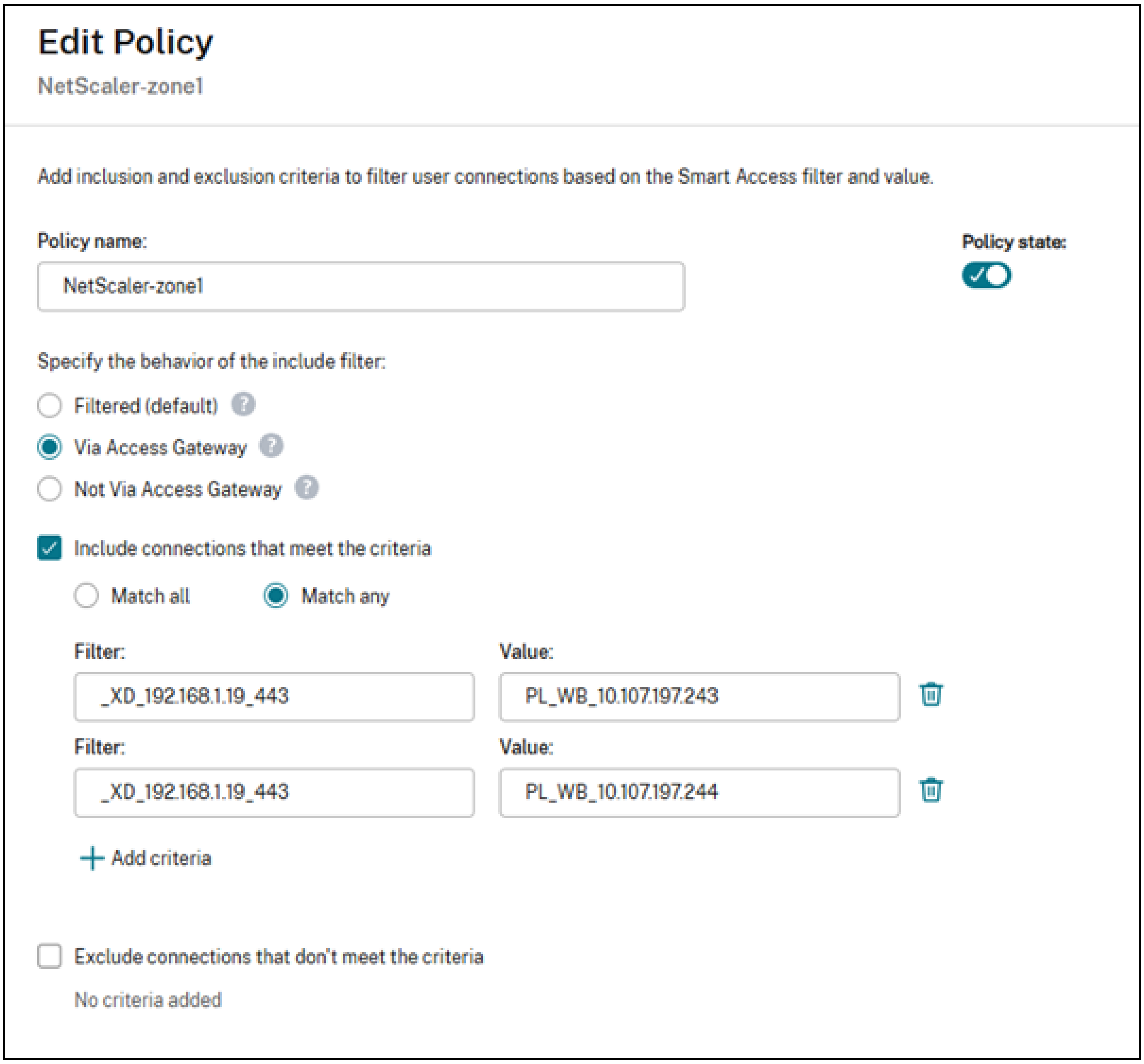
Path:

Path type: File

6. Filter enumerated resource results by Smart Access

We support the viaAG broker access rules.

Assume we've got an existing access policy as below:



Edit Policy

NetScaler-zone1

Add inclusion and exclusion criteria to filter user connections based on the Smart Access filter and value.

Policy name: NetScaler-zone1

Policy state: ✓

Specify the behavior of the include filter:

○ Filtered (default)

● Via Access Gateway

○ Not Via Access Gateway

☑ Include connections that meet the criteria

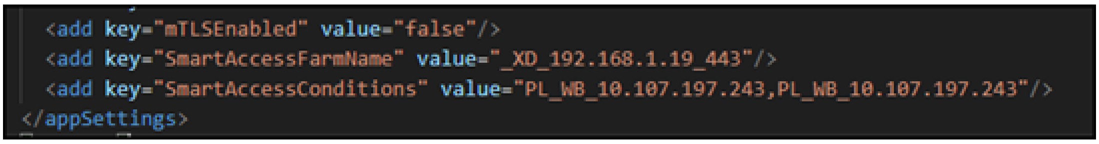
○ Match all ● Match any

Filter:	Value:
_XD_192.168.1.19_443	PL_WB_10.107.197.243
_XD_192.168.1.19_443	PL_WB_10.107.197.244

□ Exclude connections that don't meet the criteria

No criteria added

Edit `Web.config`:



```
  <add key="mTLSEnabled" value="false"/>
  <add key="SmartAccessFarmName" value="_XD_192.168.1.19_443"/>
  <add key="SmartAccessConditions" value="PL_WB_10.107.197.243,PL_WB_10.107.197.243"/>
</appSettings>
```