Citrix Session Remote Start

Contents

Introduction 2

Installation of Session Remote Start 4

Certificates 4

Configure Session Remote Start 8

Configure Citrix Virtual Apps and Desktops REST API Credentials 14

StoreFront Configuration 19

Configure DDC 24

Configure Logon script for AD server 25

Configure Citrix FAS 29

Telemetry 30

Installation checklist 32

Verify Session Remote Start API Calls 36

Session Remote Start local testing 39

NetScaler for Load Balancing Multiple Session Remote Start Servers 52

FAQ 60

Known issues 61

Optional Configurations 62

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Introduction

February 12, 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.

> **Note:**
>
> Session Remote Start is currently in Public Tech Preview. Contact Citrix sales for details about the general availability.

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.

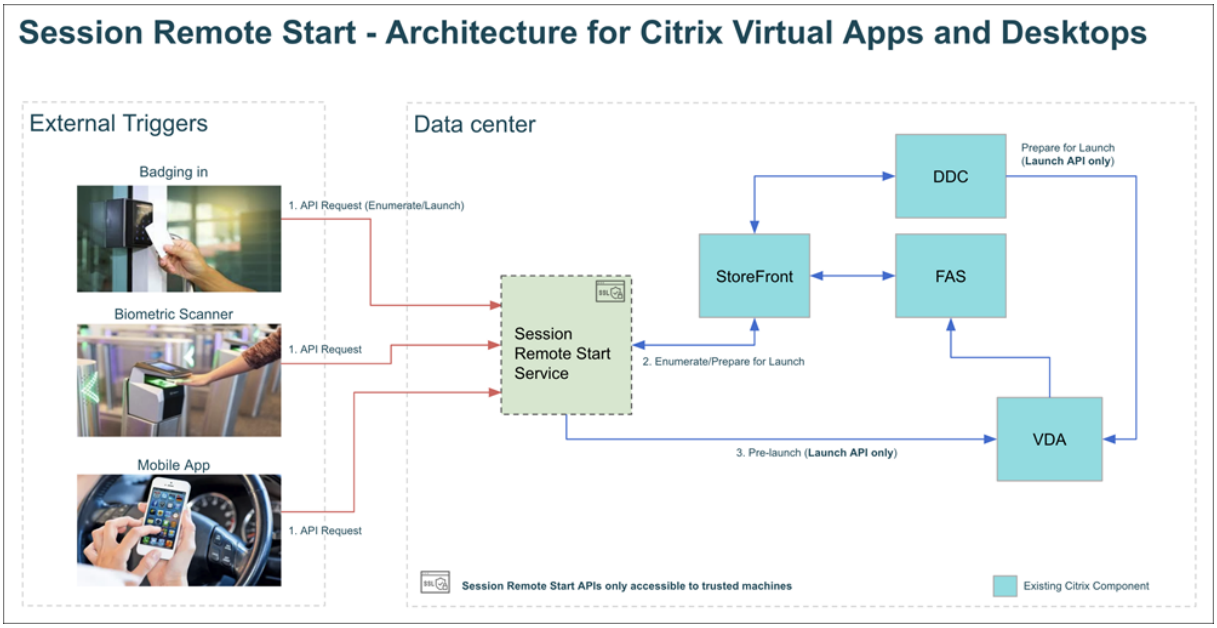
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

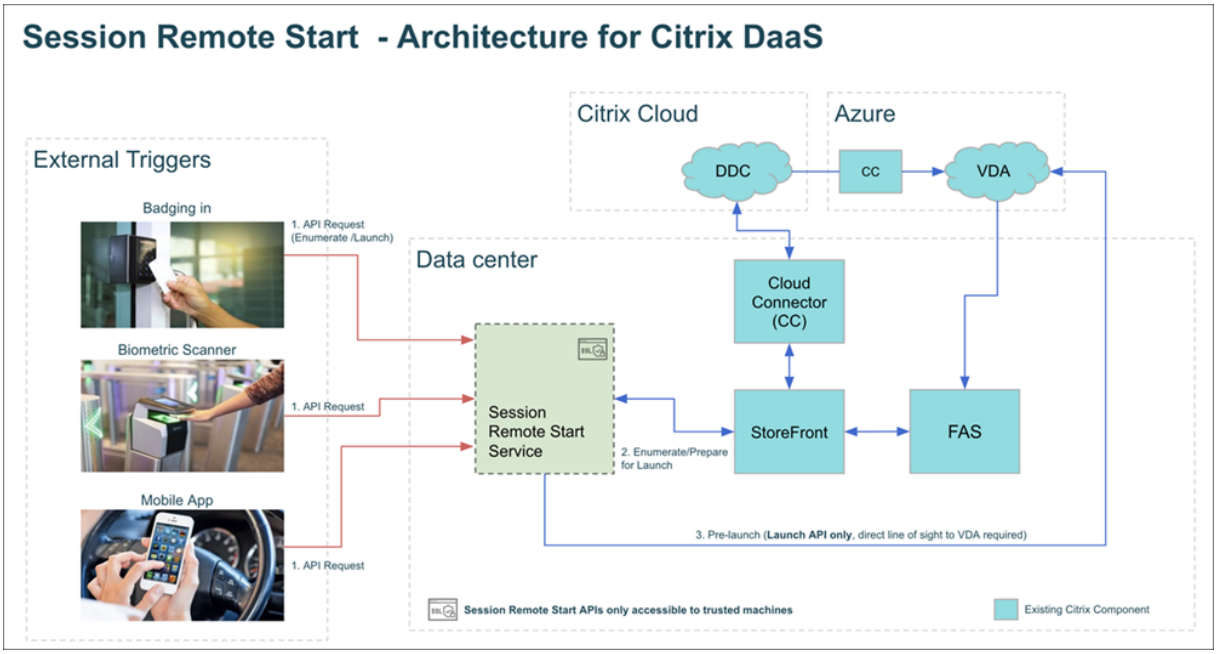
> **Important Note:**
>
> Session Remote Start works with Citrix Virtual Apps and Desktops on-prem and Citrix DaaS when StoreFront is used. Currently, Session Remote Start does not work with Citrix Workspace (Cloud version of StoreFront). StoreFront is a requirement for Session Remote Start.

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.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

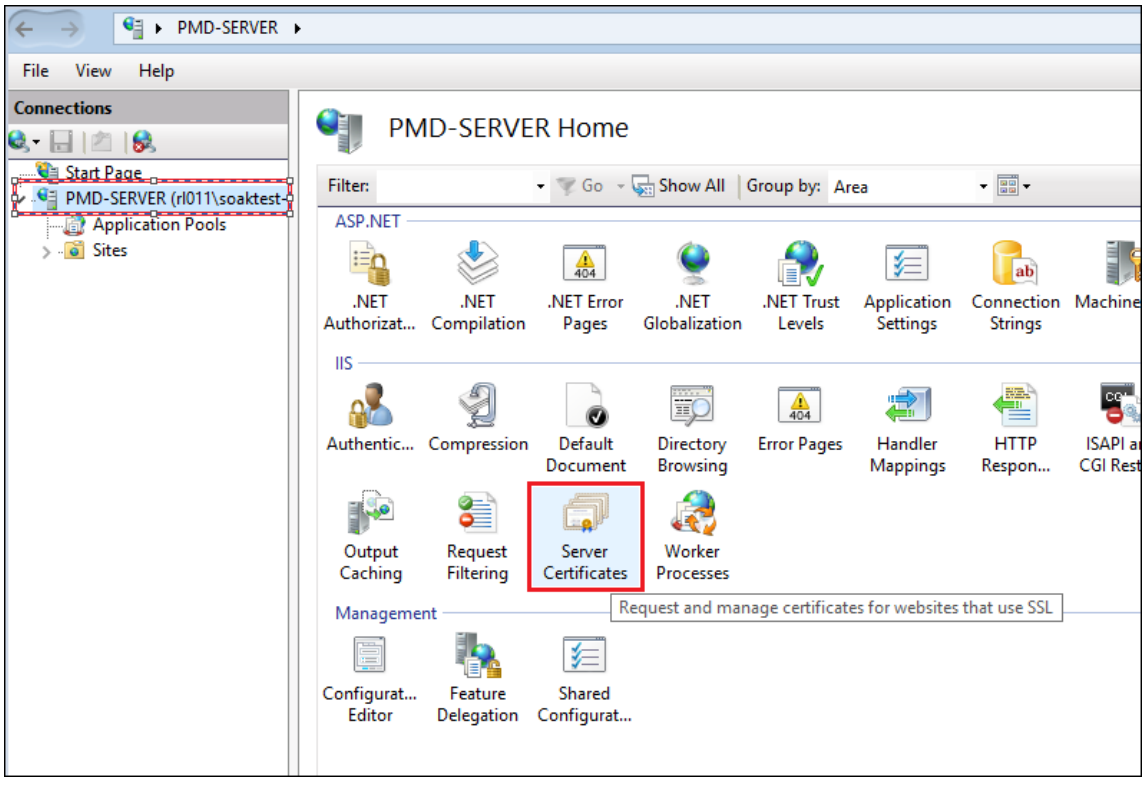
The **IIS identity** under which Session Remote Start is running must be able to visit the StoreFront URL of **Receiver for Web Site** without warning. (For example, `https://storefront.rl011.local/Citrix/srsWeb`)

Import Server SSL certificate to IIS Manager

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

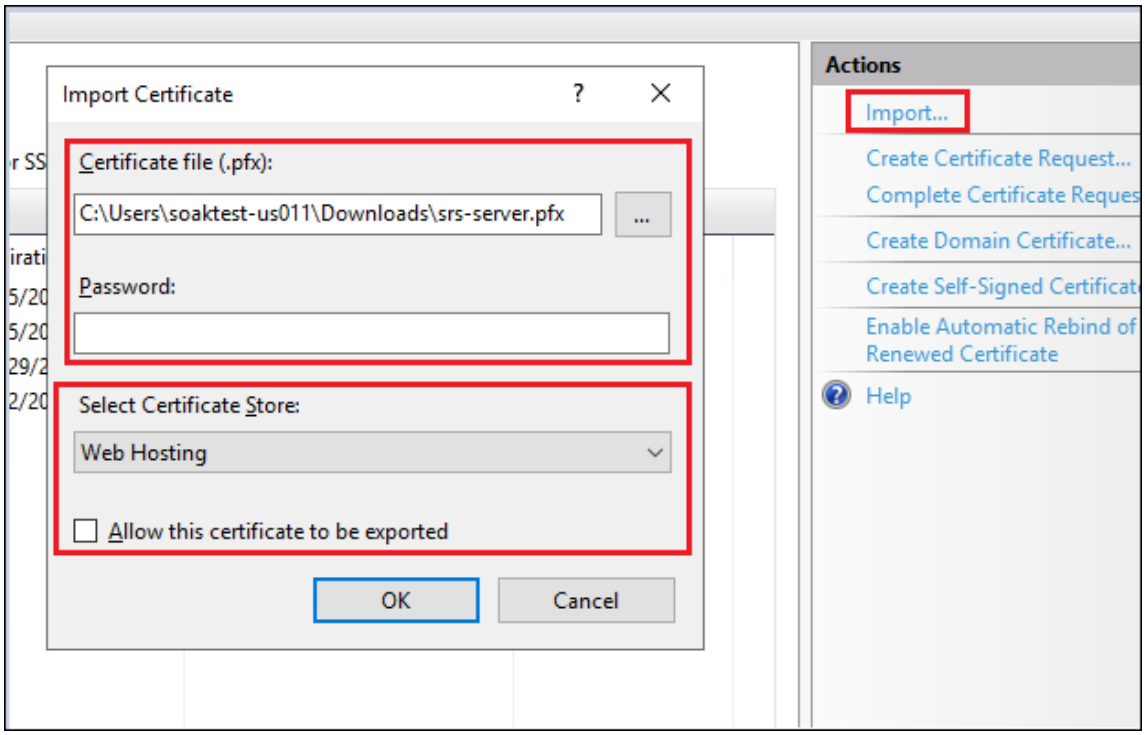
Securing access and encrypting traffic with SSL certificates is the preferred way of deploying Session Remote Start. The secure access and encrypt traffic with SSL certificates:

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



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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



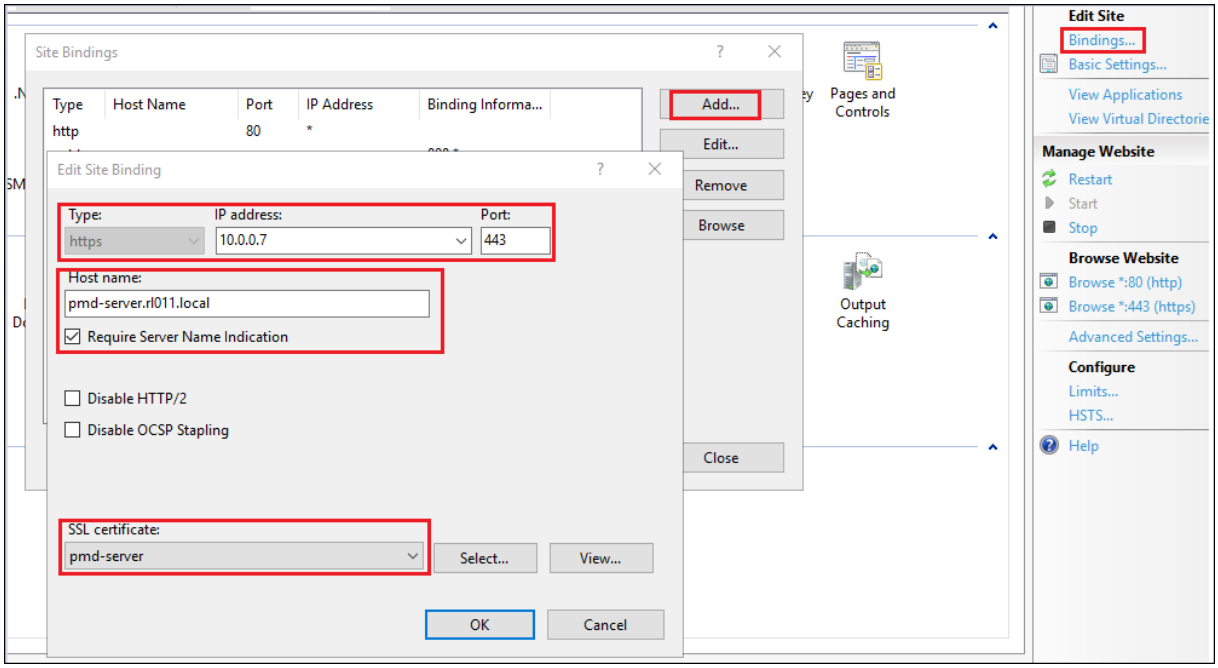
Make sure the Session Remote Start service IIS identity has the necessary permissions to load the certificate. The settings shown for **Certificate store** and **Allow this certificate to be exported** in the images are recommended for better security. If **Web Hosting** is selected, remember to import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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



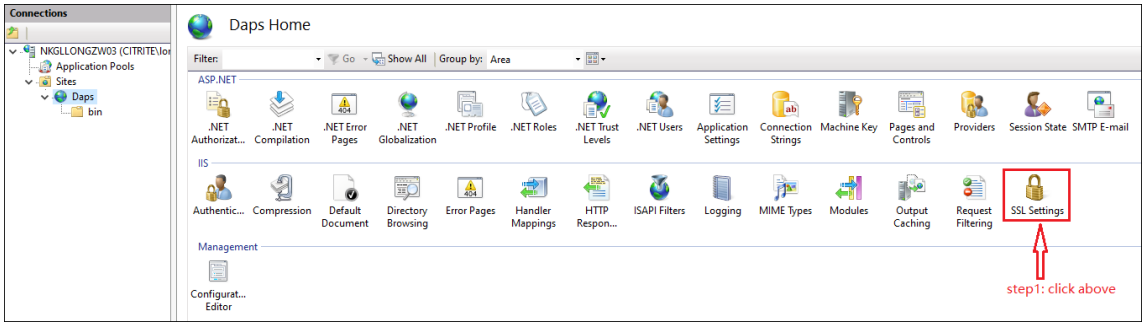
1. On the IIS Manager, click **Default Web Site** under **Sites**. On the right panel, under **Actions > Edit Site**, click **Bindings**.
2. Click **Add**.
3. Under the **Add Site Binding** screen.
    - Select the type as **https**.
    - Set https port to **443**.
    - Enter the IP address and host 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.

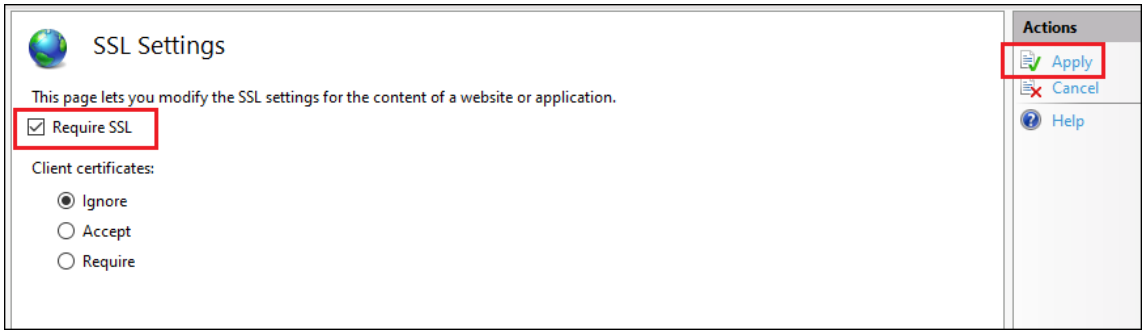
Require SSL

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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



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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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`

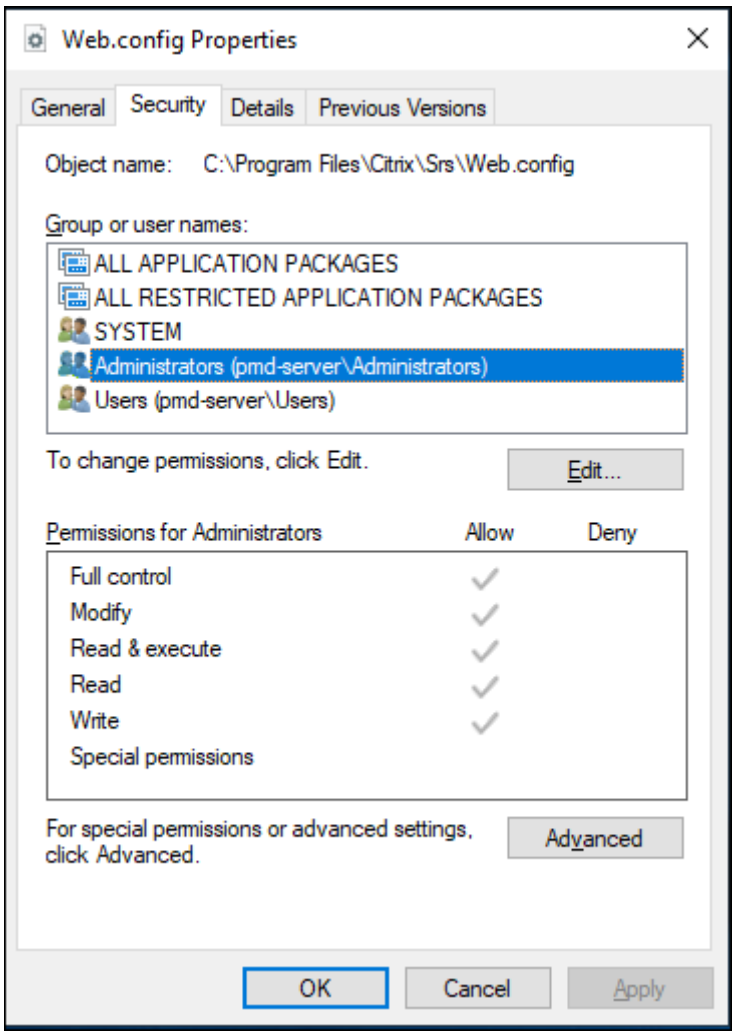
For log-related configuration, please refer to the Log file Configuration section.

Configuration file permissions

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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



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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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.

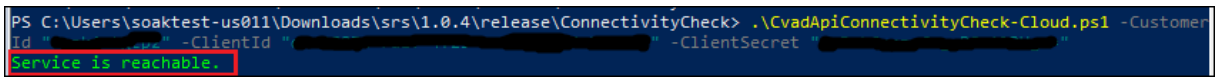
Confirm that Session Remote Start server can connect to Citrix Virtual Apps and Desktops REST API Service

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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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



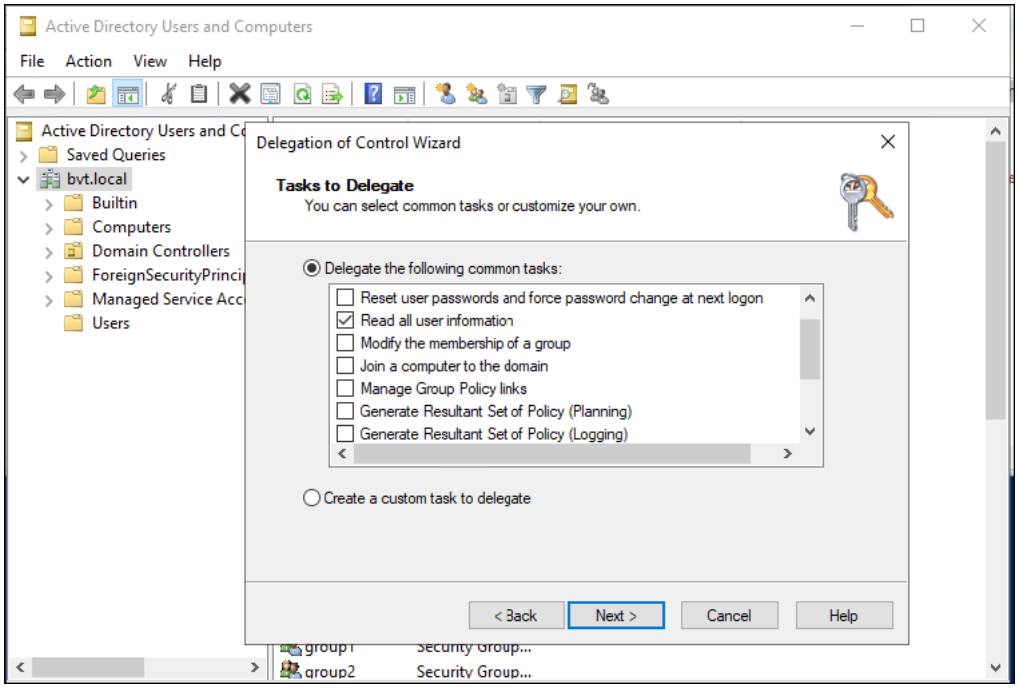
Create a user and store the Citrix Virtual Apps and Desktops REST API credentials

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.

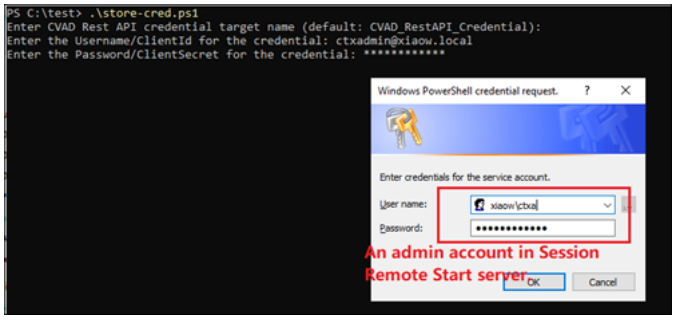
Domain user On the Domain Controller, create or use an existing Domain Service Account with the **Read all user information** permission delegated.

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**.



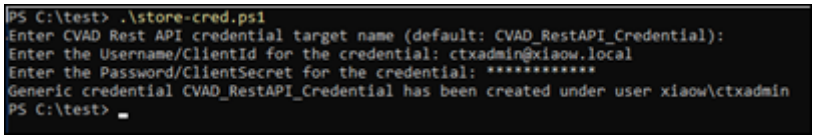
4. On the Session Remote Start server, navigate to the **SessionRemoteStart** folder in the installation package. Run the PowerShell script `store-cred.ps1` as an administrator to configure the CVAD REST API credentials.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.

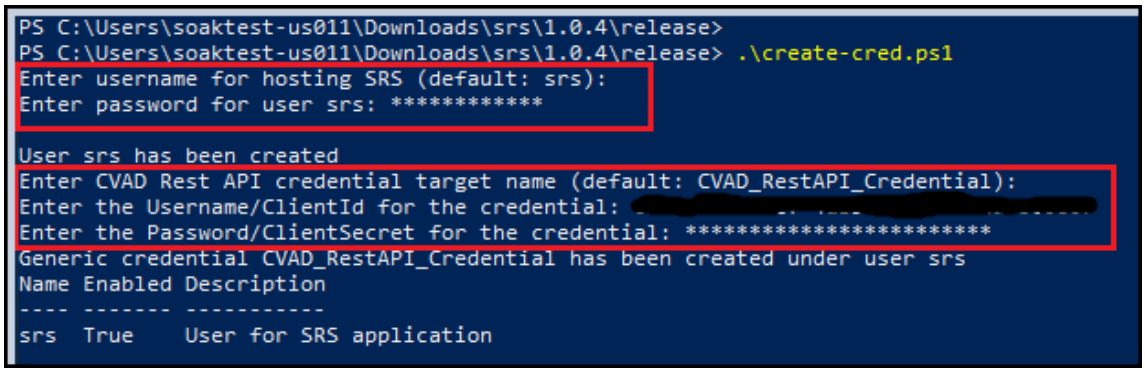
A success message is displayed upon completion.



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)



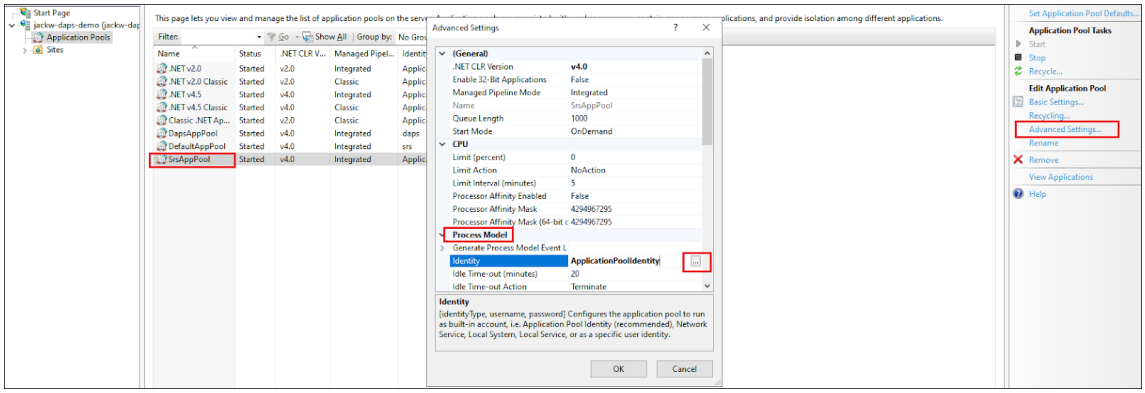
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Configure Session Remote Start Application Pool

Overview

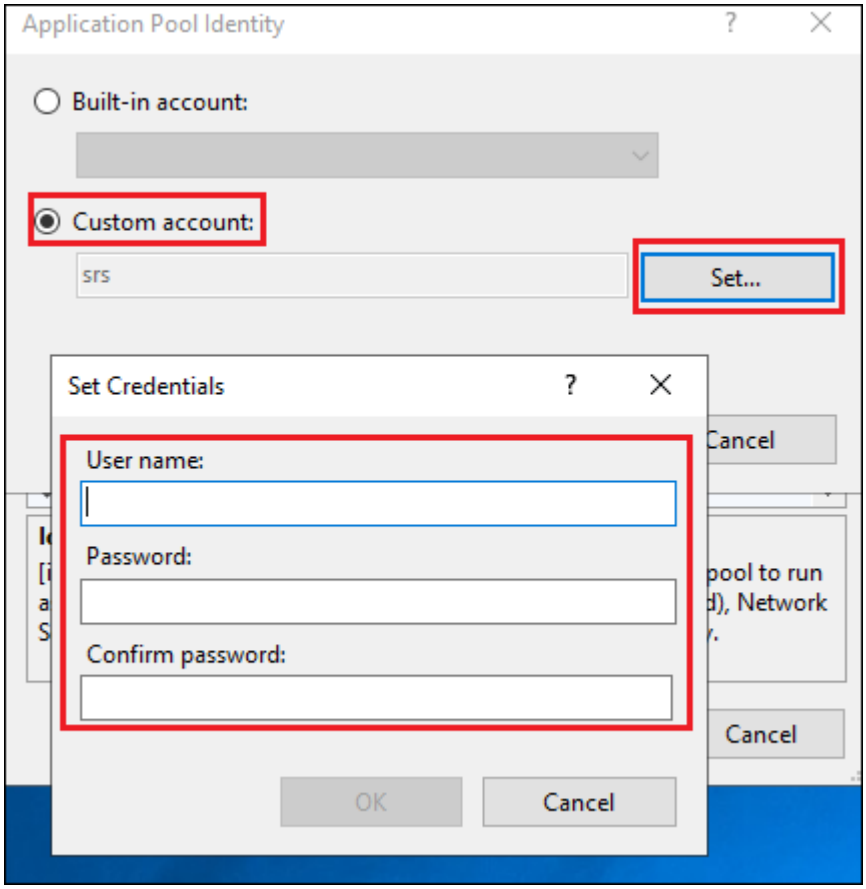
By default, IIS runs an application (site or service) under the **ApplicationPoolIdentity** for each unique application pool. Configure Session Remote Start to run under the previously created user identity by setting the Session Remote Start application pool to use the custom user:

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.



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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



> **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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

StoreFront Configuration

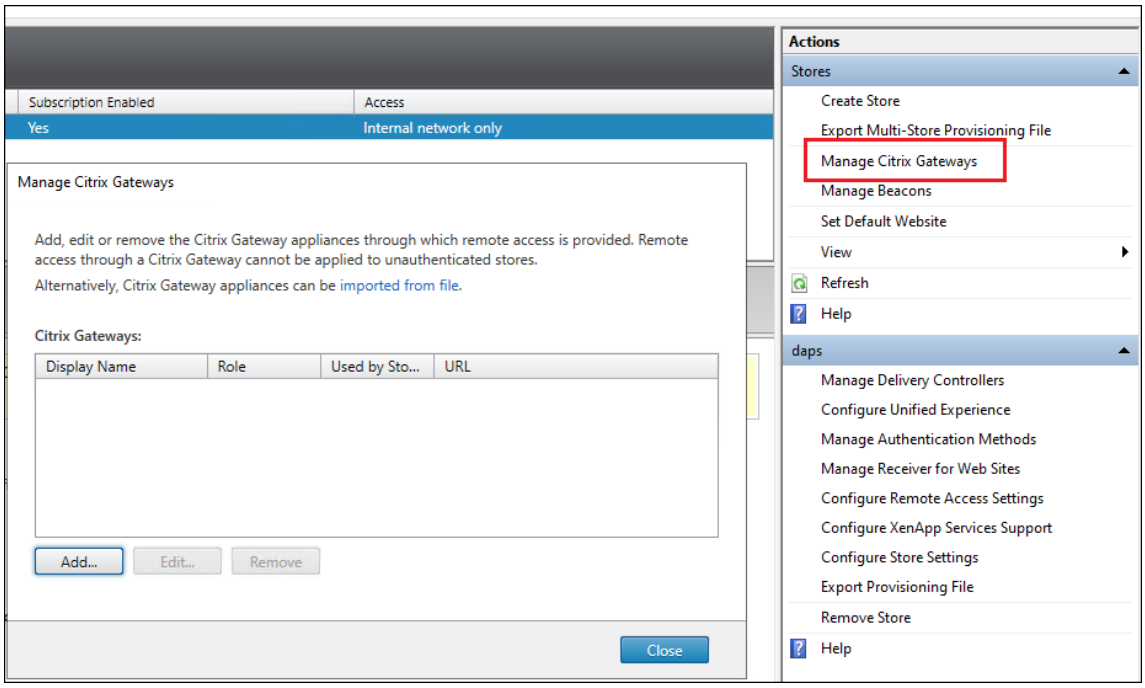
December 11, 2024

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`).

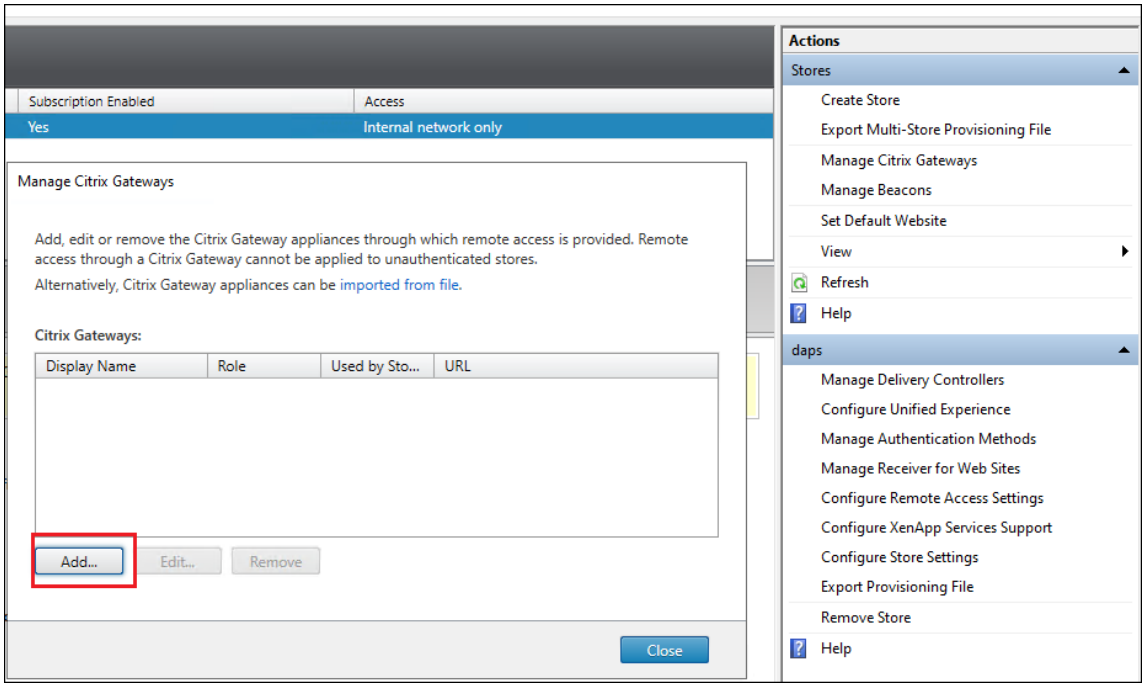
Add Session Remote Start as a Gateway

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

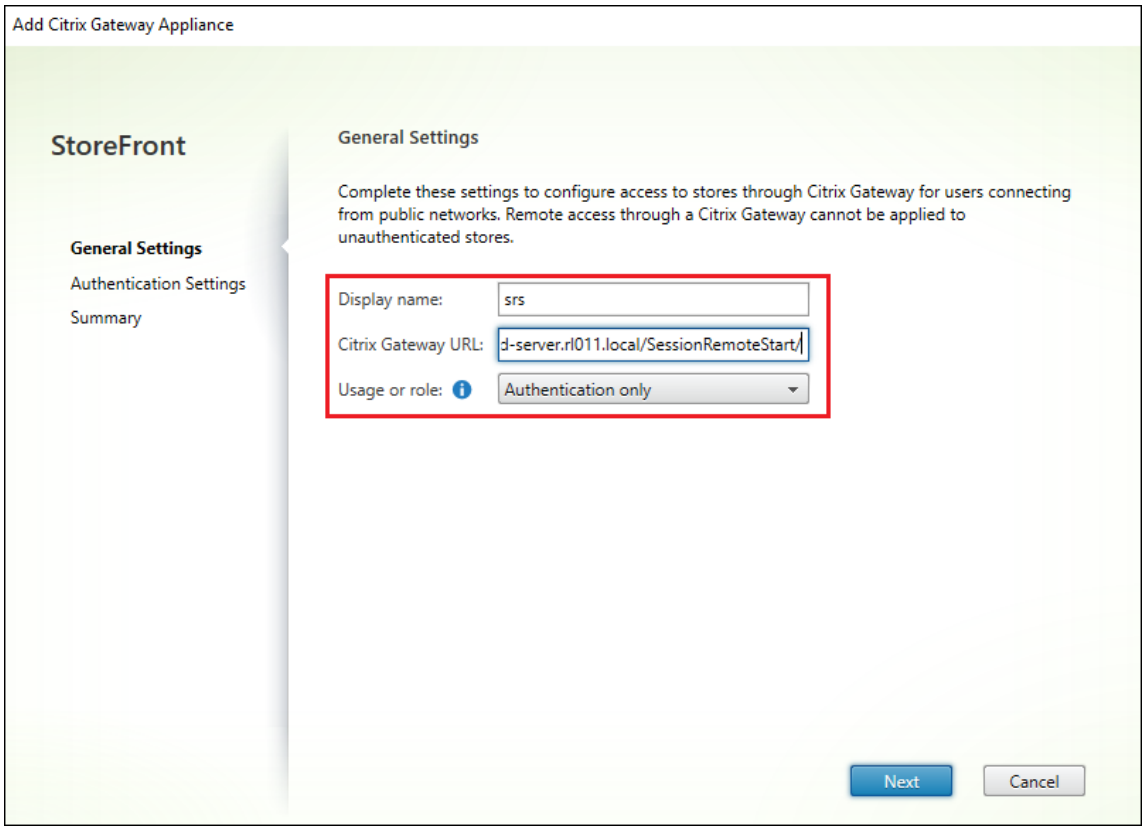


2. Add a new gateway.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



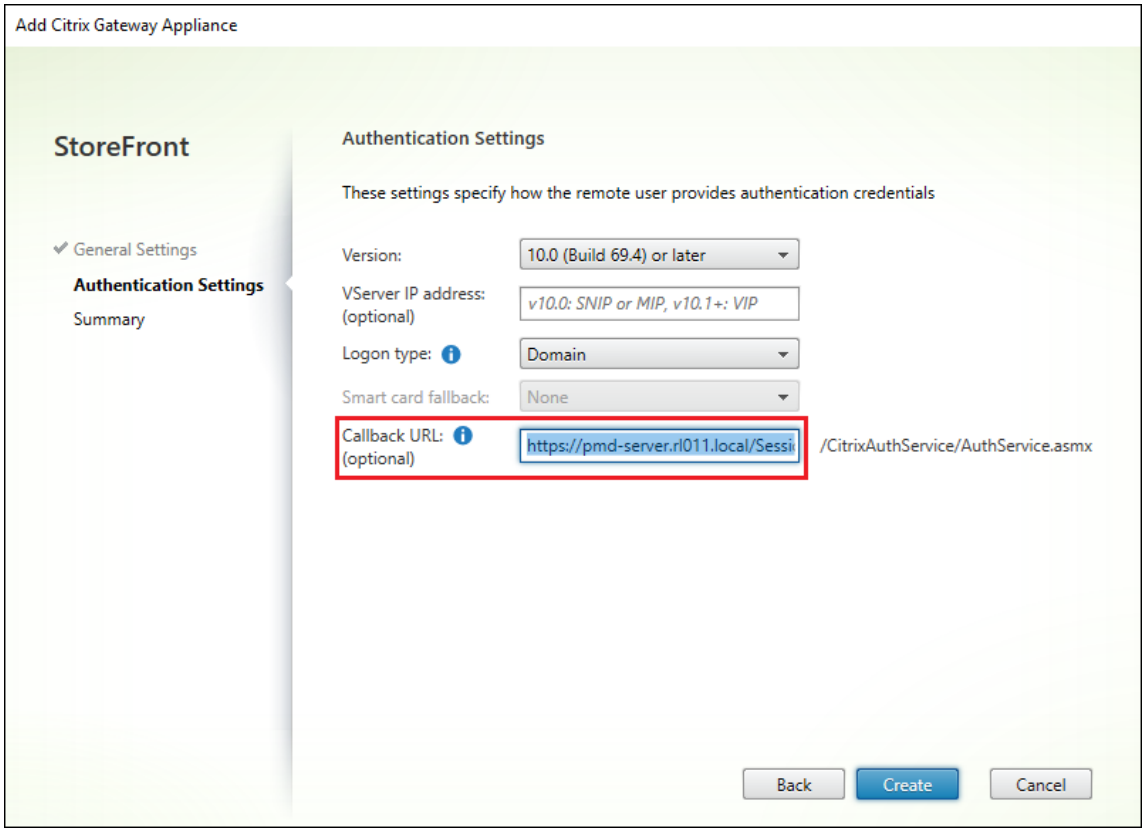
3. Set Display name, set Citrix Gateway URL with `https://<Session Remote Start FQDN>/SessionRemoteStart/`, and change **Usage or role** to **Authentication only**.



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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

.



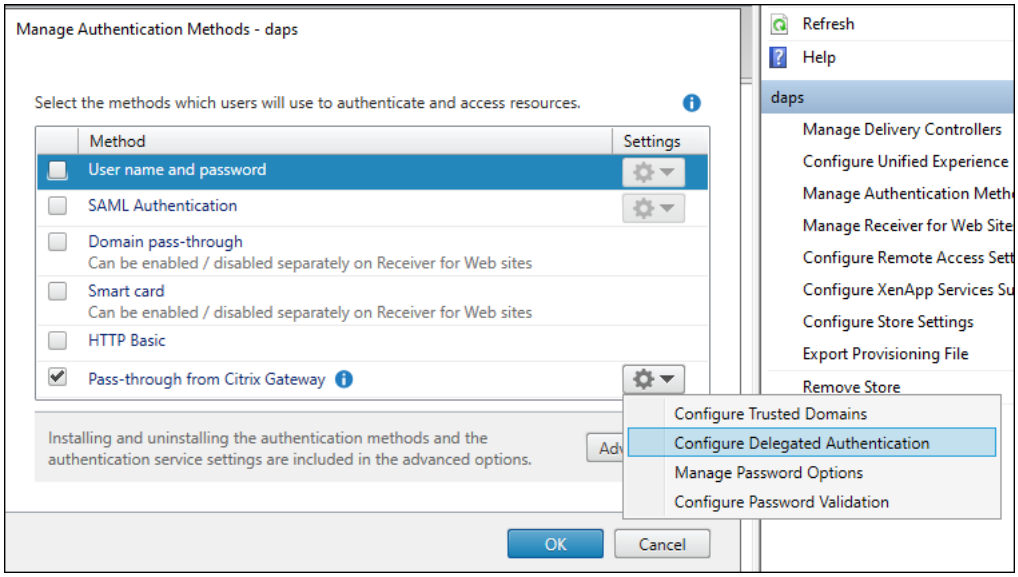
Create a New Store for Session Remote Start

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

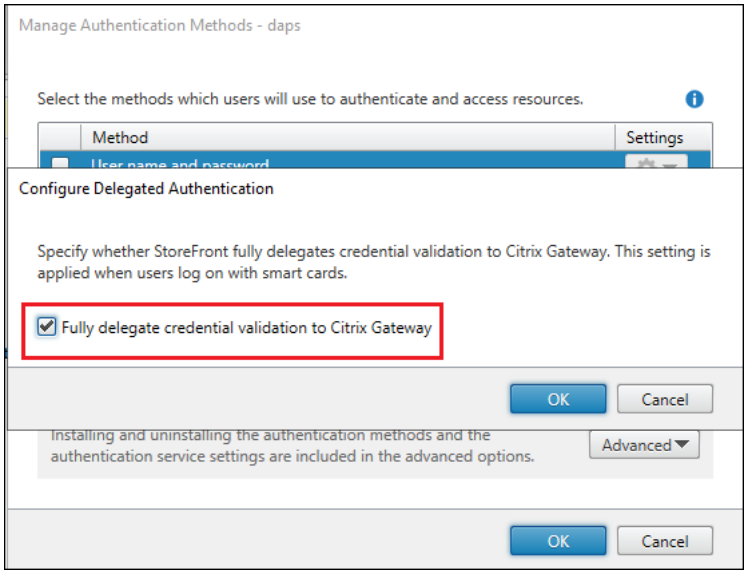
Manage Authentication Methods

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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



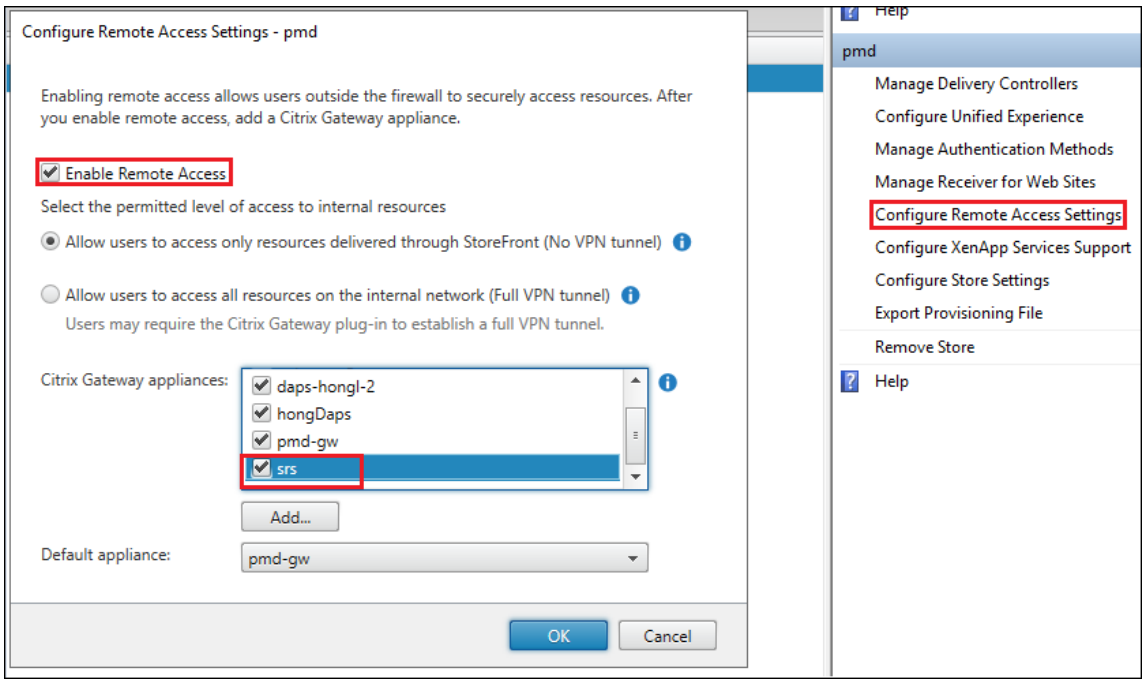
4. Enable the **Full delegate credential validation to Citrix Gateway**.



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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Variable Name	Required/Optional	Description	Example
`srs_server_urls`	Required	Session Remote Start server URL	`https://pmd-server.rl011.local/SessionRemoteStart`
`stf_original_plugin_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
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

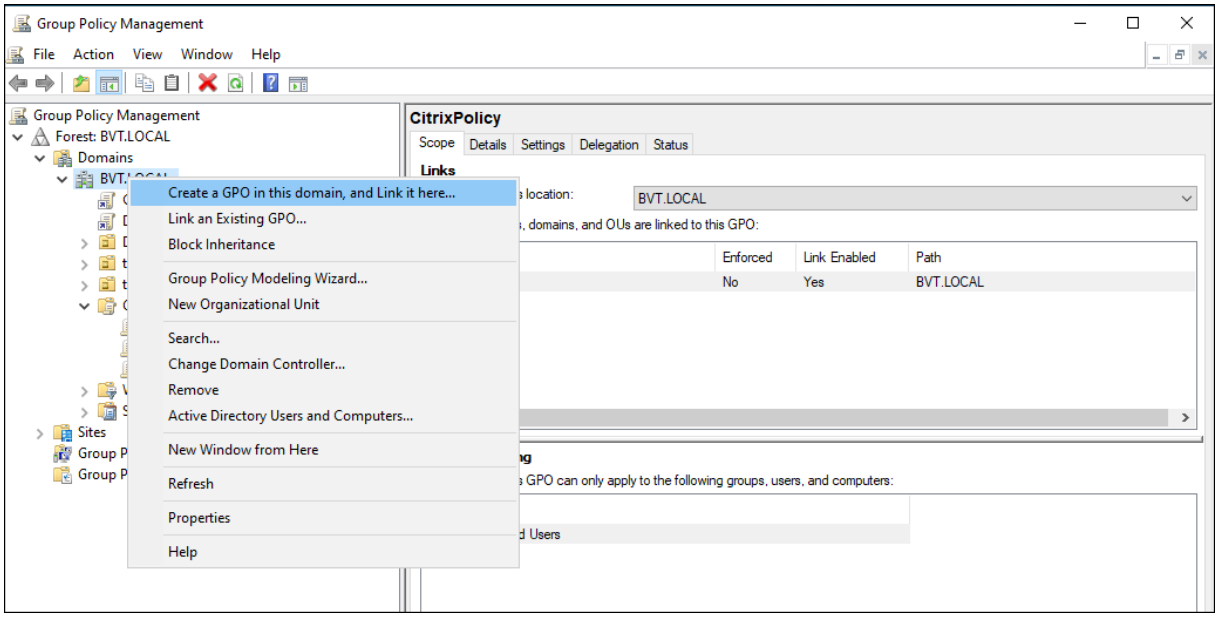
December 11, 2024

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.

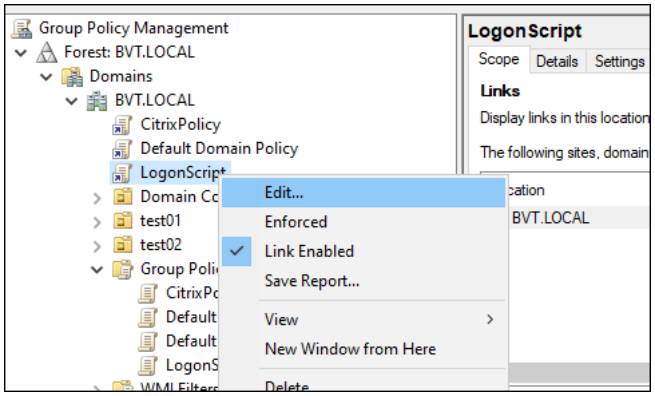
Steps to create a GPO and link it to a Domain

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

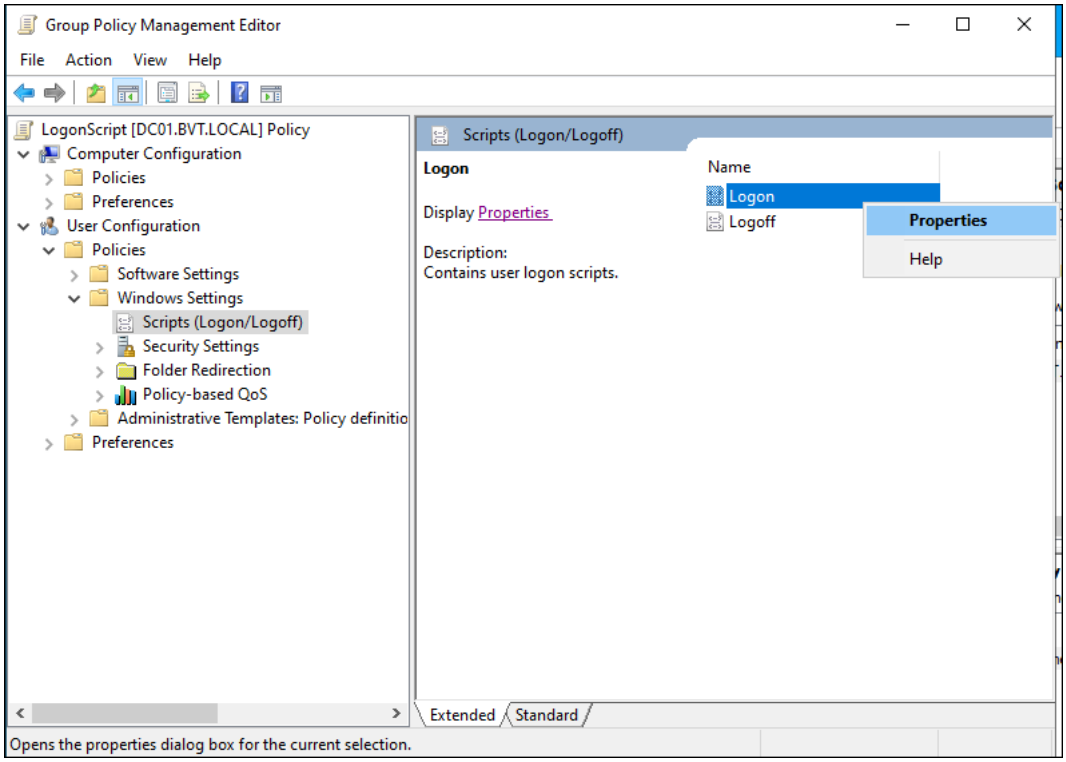


1. Right-click on the GPO, select **Edit** to open the Group Policy Management Editor.

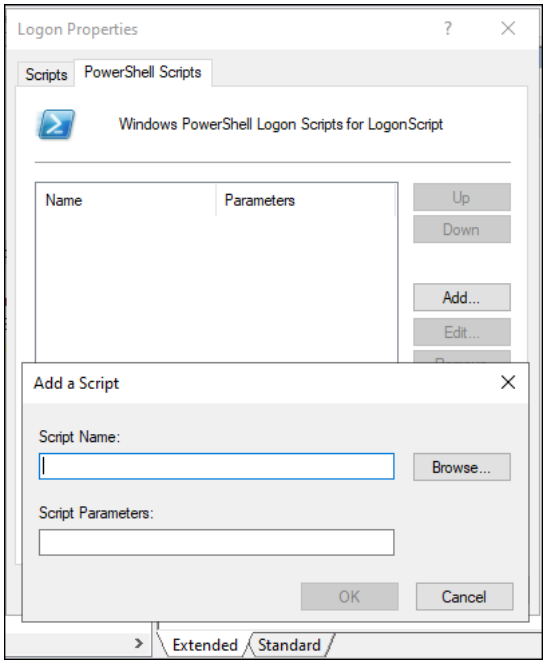


1. In the **Group Policy Management Editor**, expand **User Configuration > Policies > Windows Settings > Scripts (Logon/Logoff)**. Right-click **Logon on** in the right panel and select **Properties**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

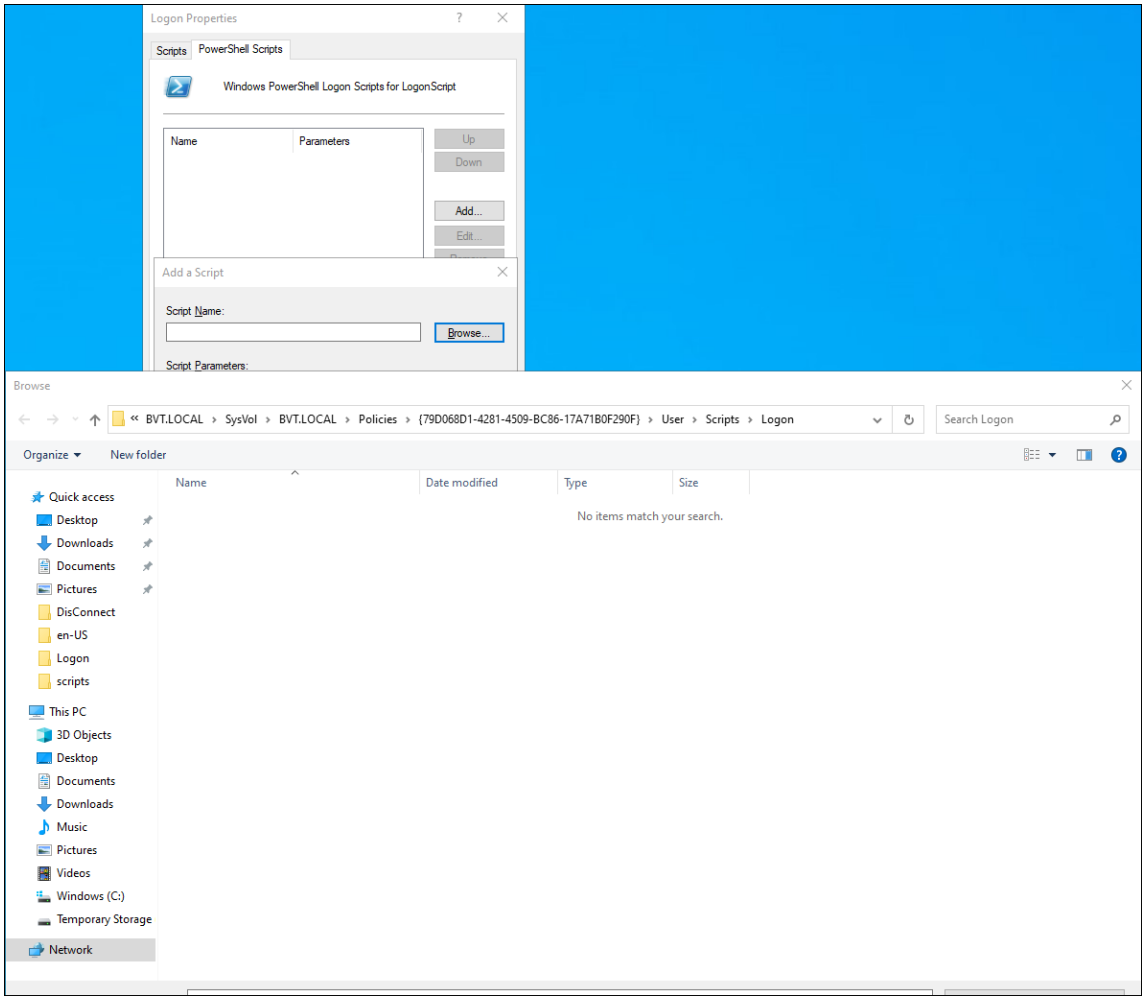


2. Switch to the **PowerShell Scripts** tab, and click **Add...**.



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

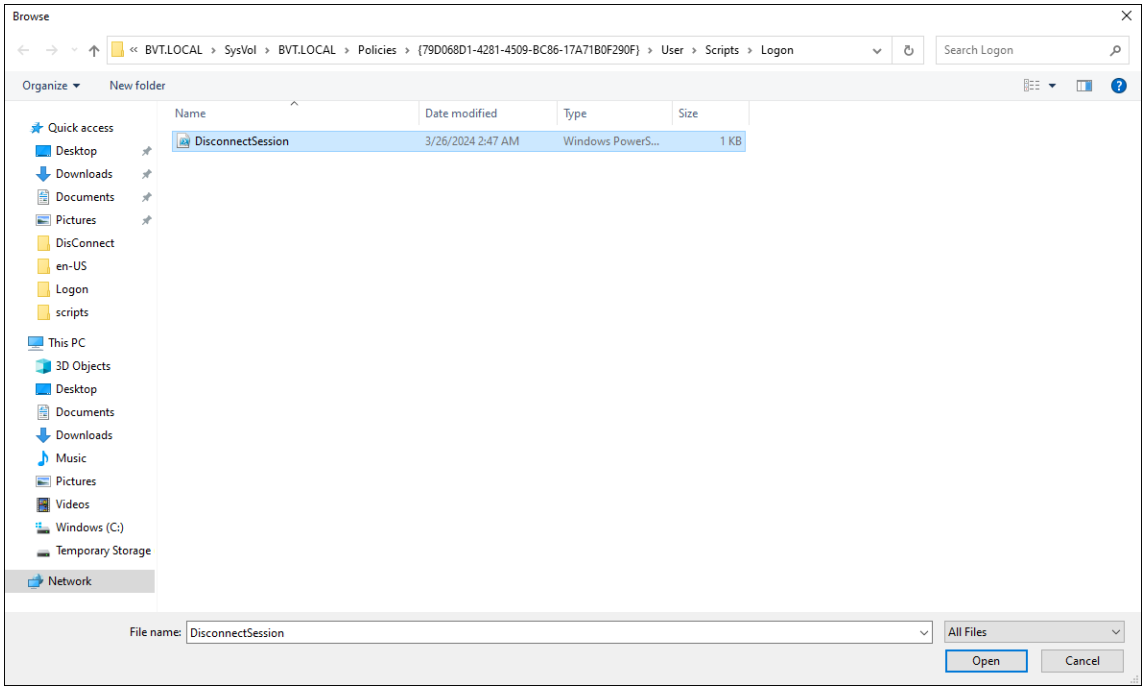
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



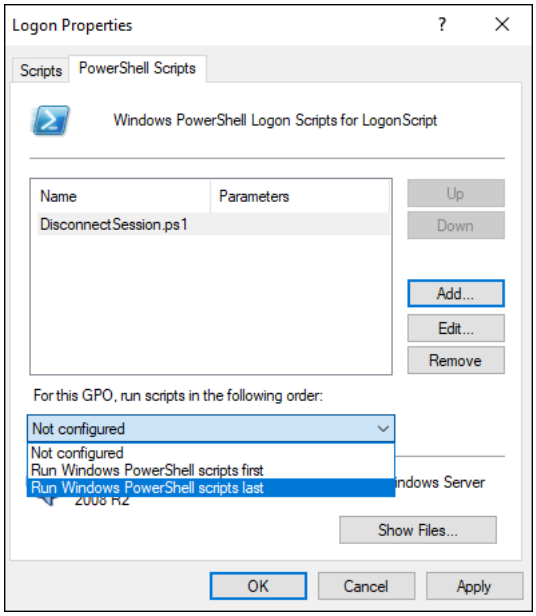
The Logon folder is a shared folder which typically has read-only and execute permissions by machines and users. To avoid permission issues, it is recommended not to use any other folder.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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



Configure Citrix FAS

December 12, 2024

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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"`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

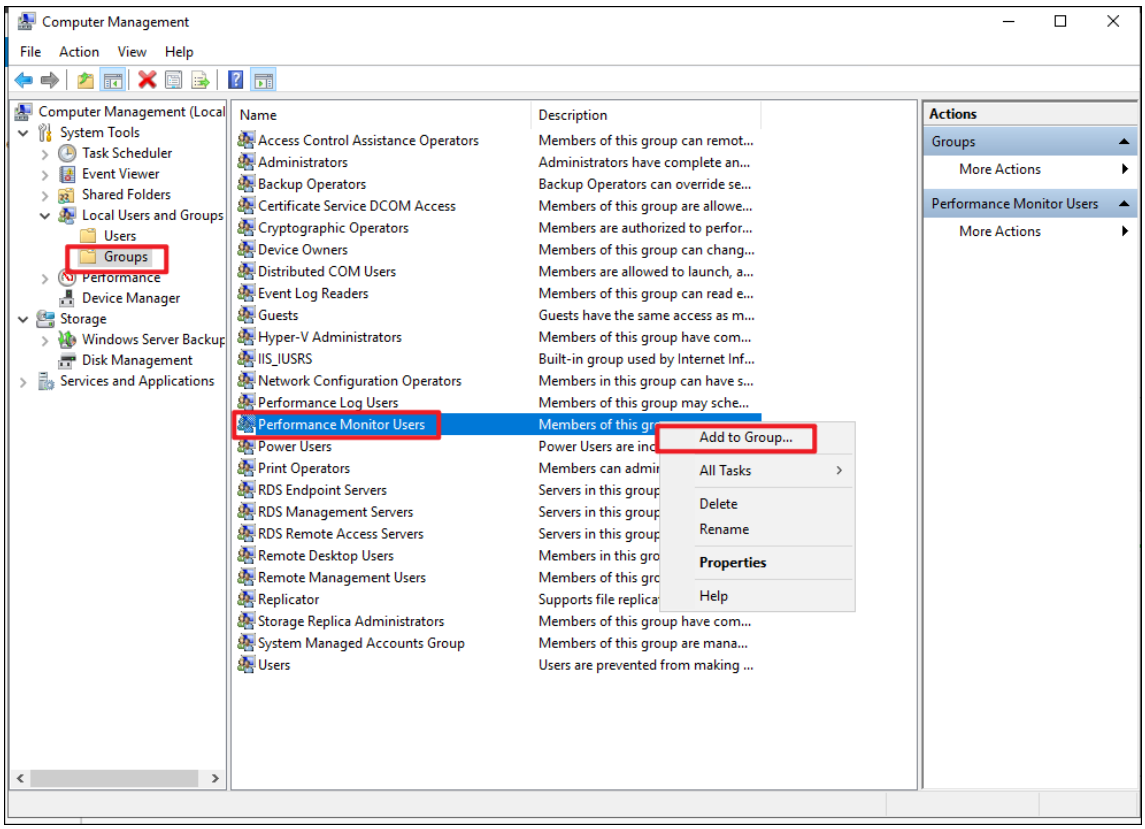
Session Remote Start server is designed to capture the following data:

- 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

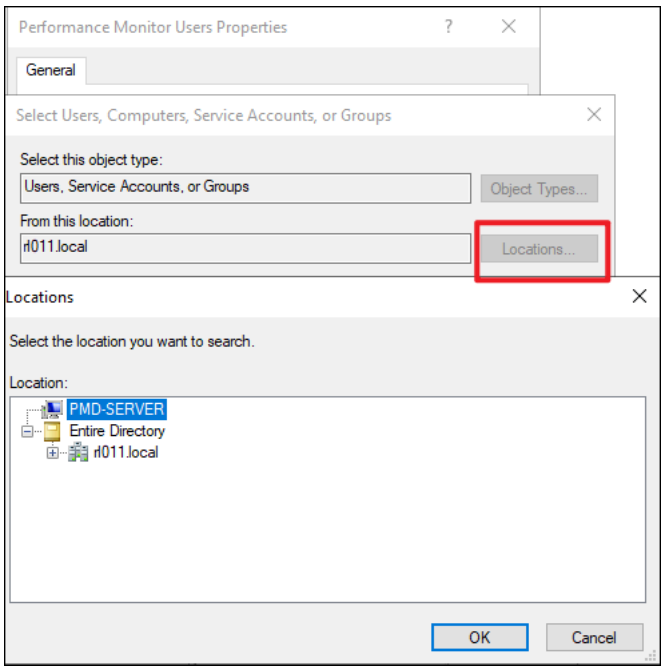
The following steps are required to make the IIS Application Pool have the permission to collect performance monitor data.

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...**.

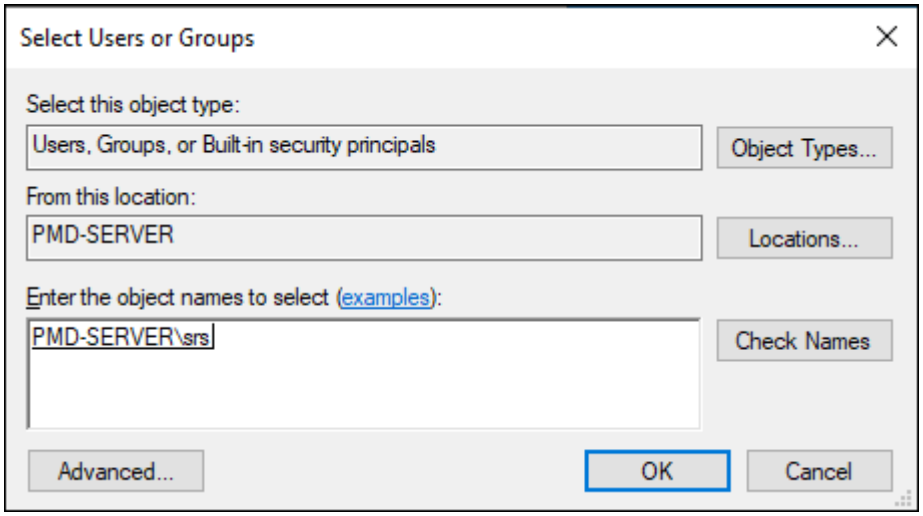


2. Click **Add..** and then click **Locations...** and select your local computer.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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



4. Open PowerShell, and run the following commandlet:

```
iisreset
```

Installation checklist

December 11, 2024

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

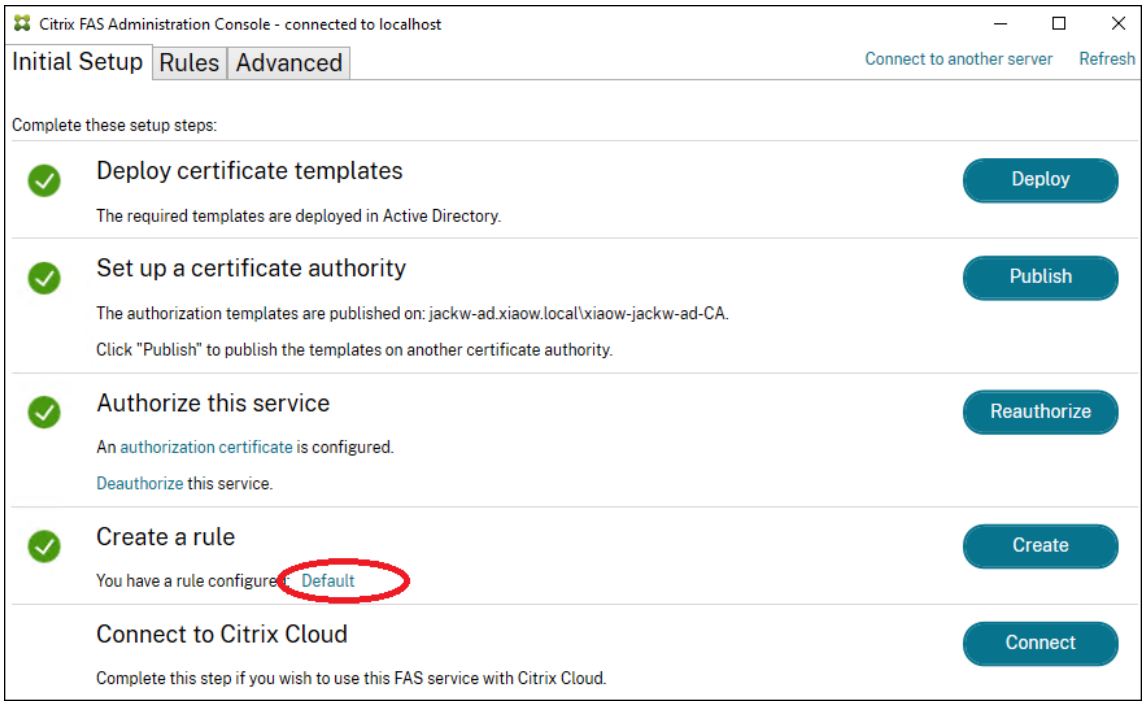
Verify if the logon script is configured.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

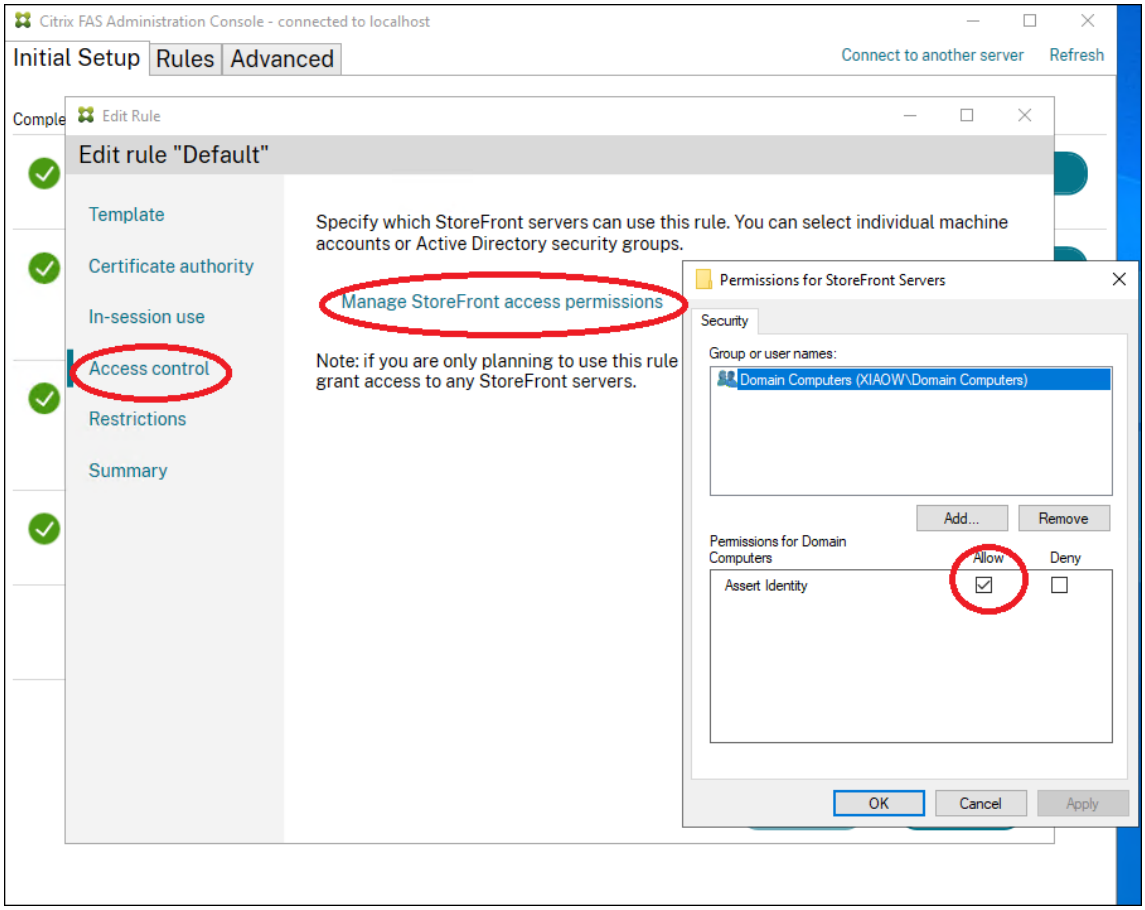
FAS

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.



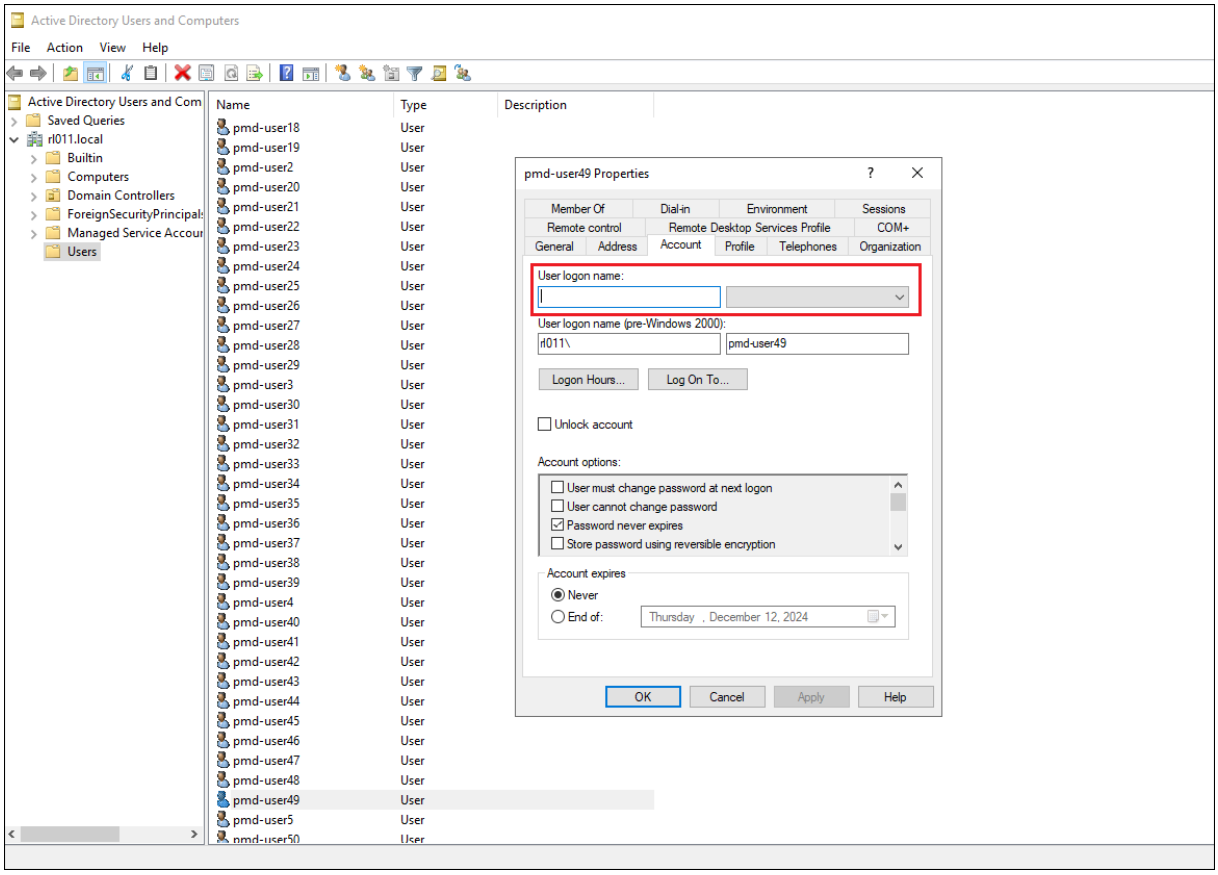
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



User Logon Name

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Example:

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

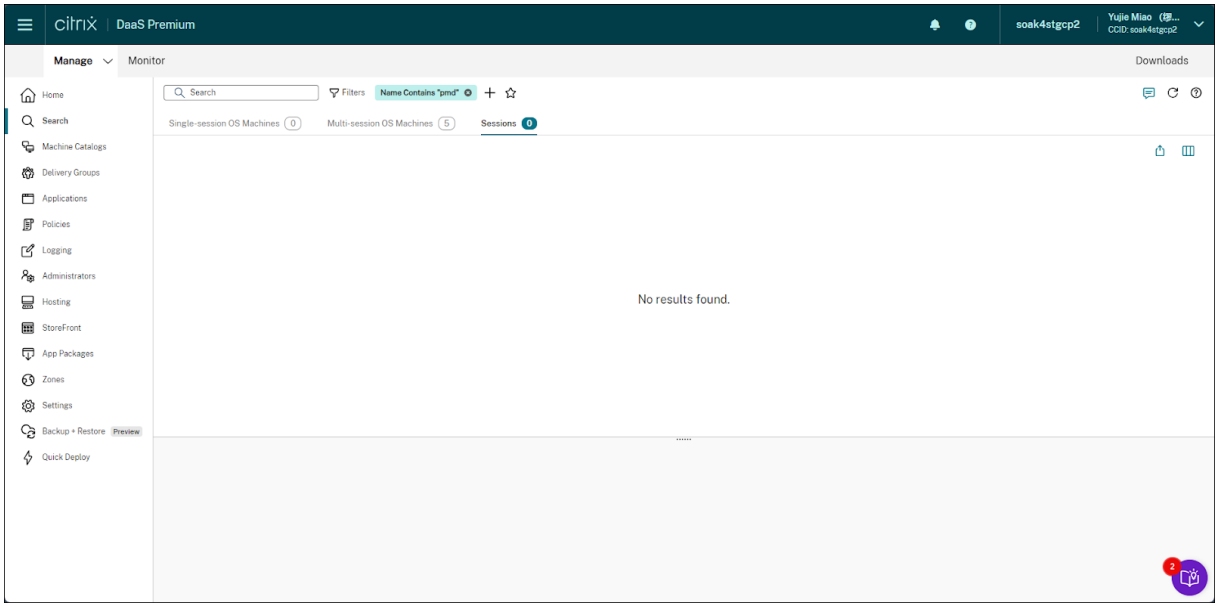
In this example, the user **pmd-user2@rl011.local** is assigned to launch desktop **PMD-Server2019-2** (this is the name of the desktop as users see on their workspace). And no target resource is specified for user **pmd-user1@rl011.local**, the script will choose the first one in the resource list.

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 ----------------------------------------------
```

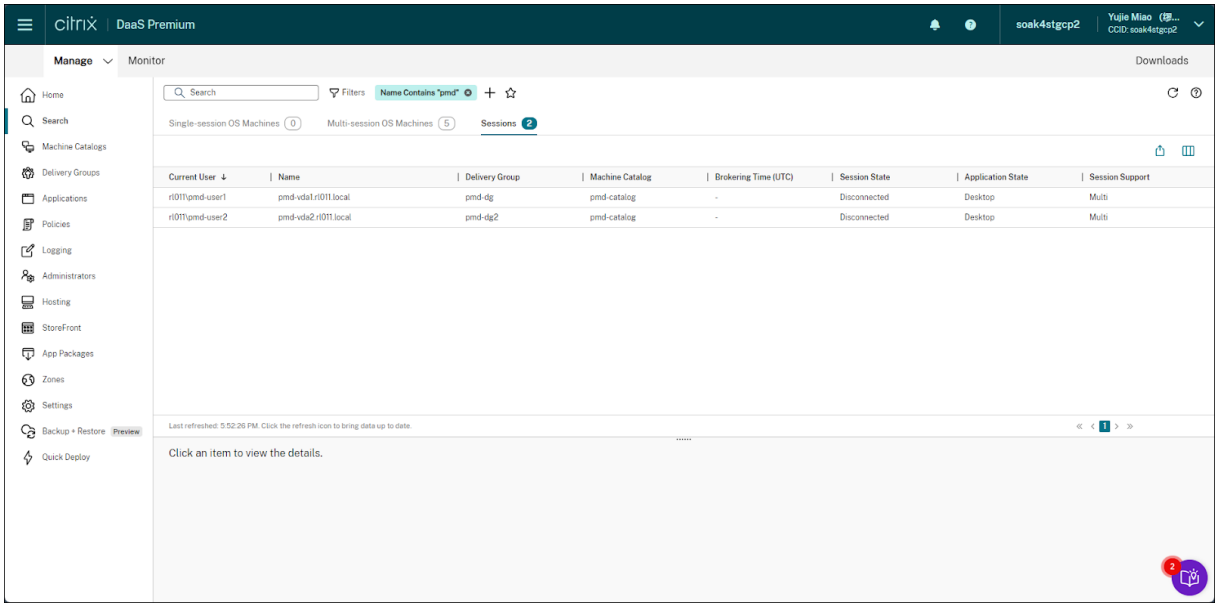
Verify the job output to make sure the resources are pre-launched successfully.

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



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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

Session Remote Start local testing

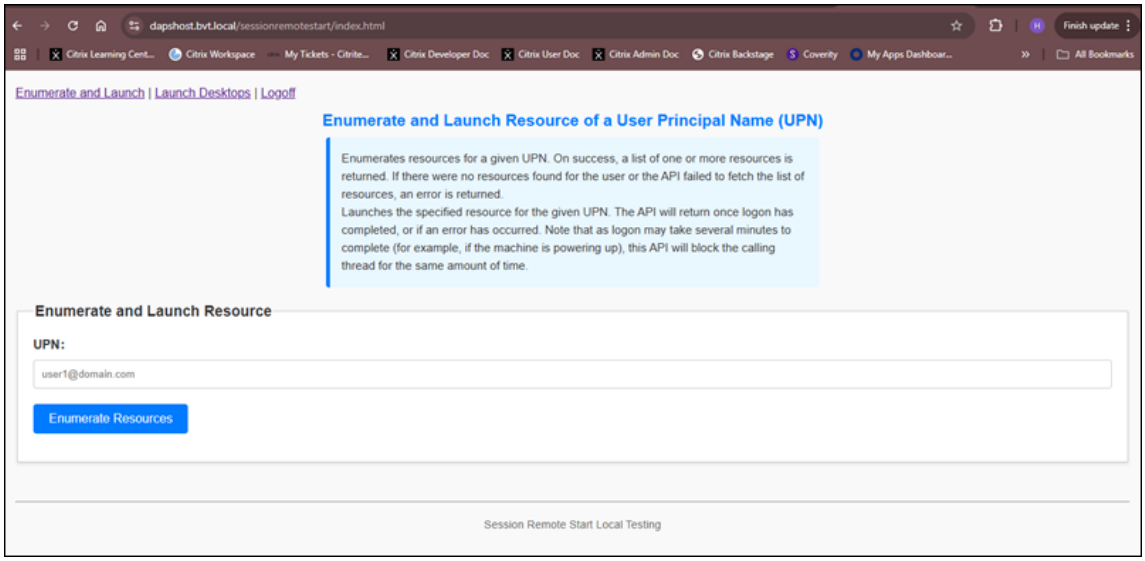
January 15, 2025

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.

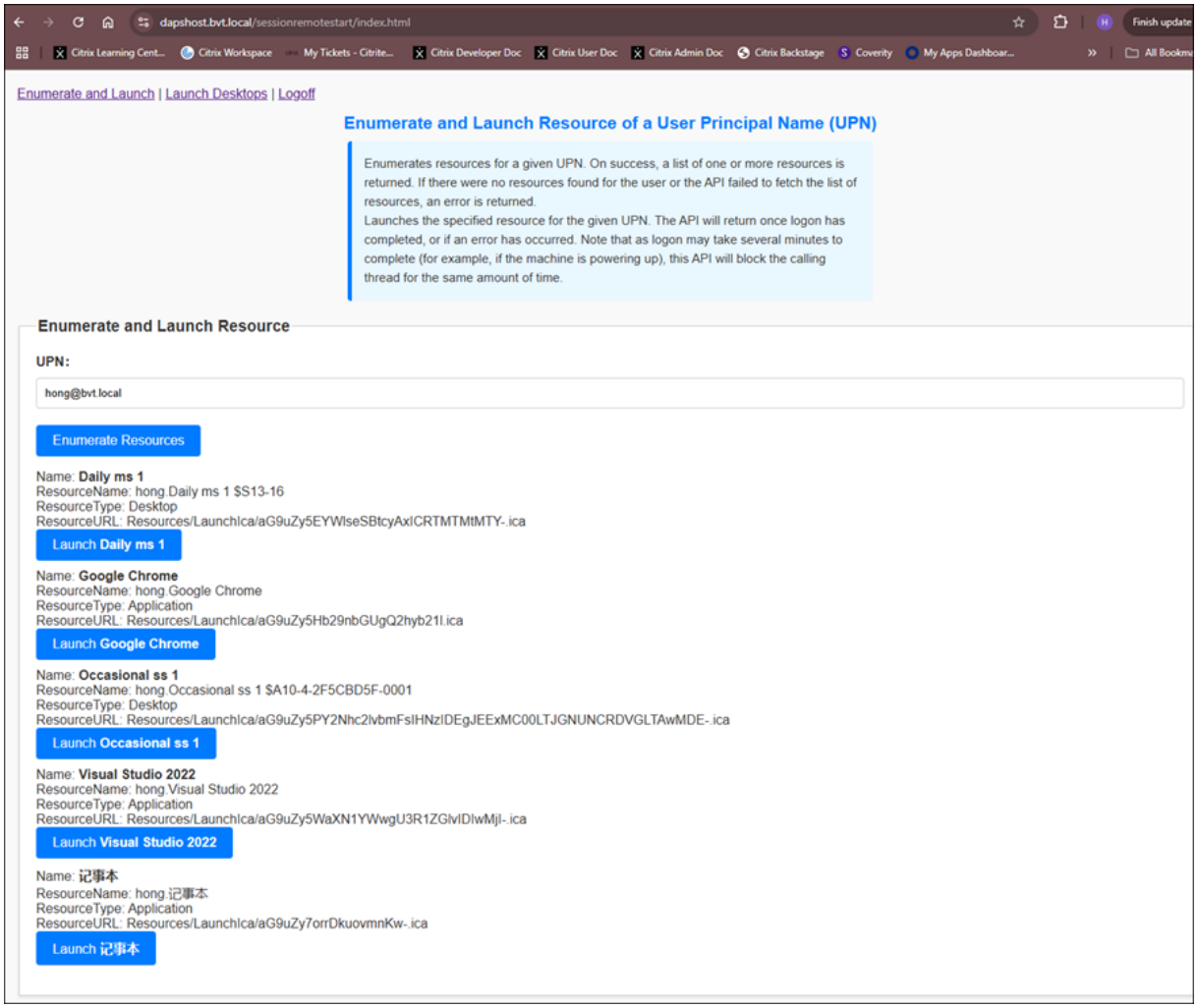
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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

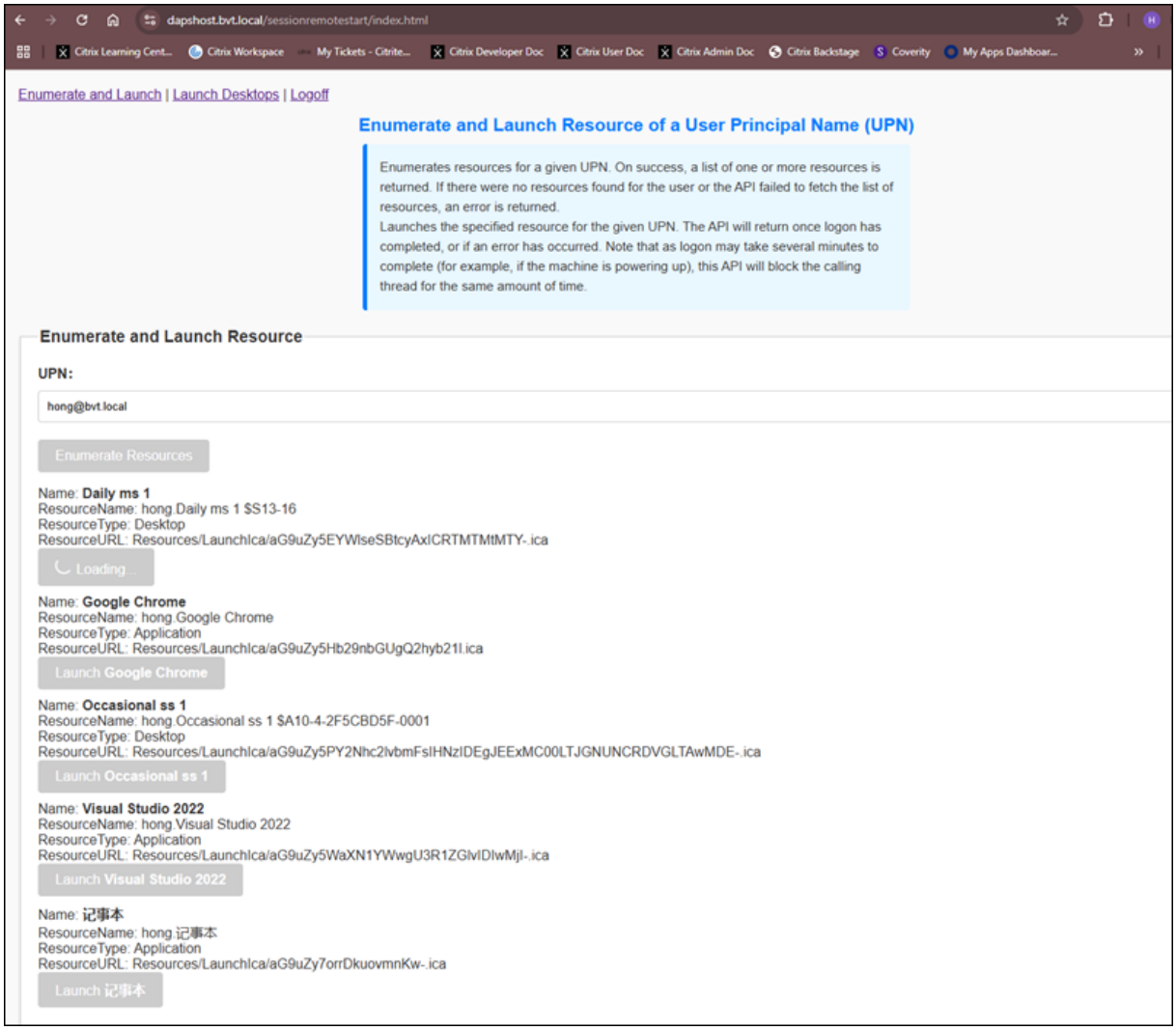
Input the User Principal Name (UPN), then click **Enumerate Resources**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



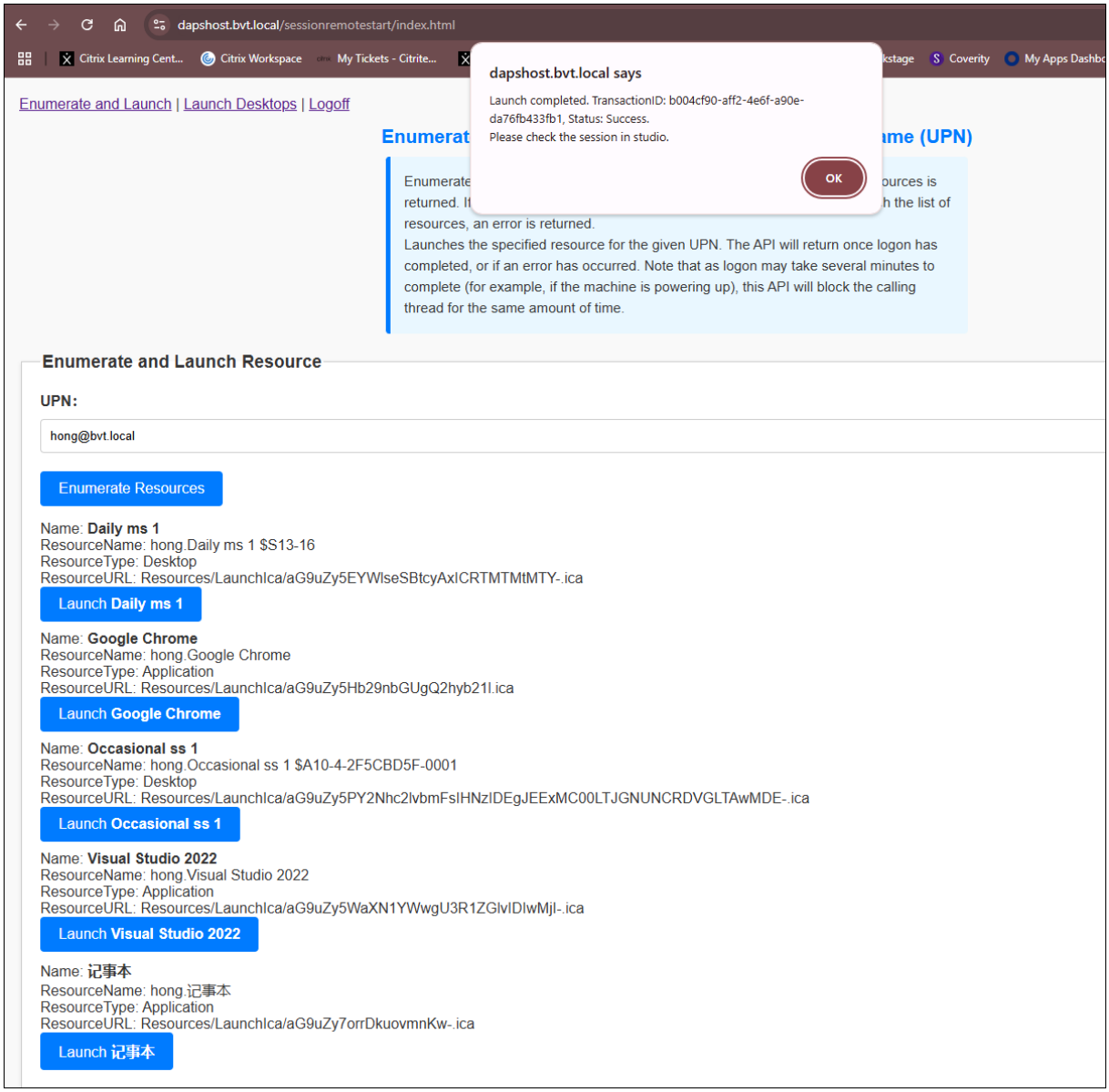
Then choose a resource, for example: `Daily ms 1` and click `Launch Daily ms 1`. The API waits for a logon notification from the VDA before returning to the caller.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

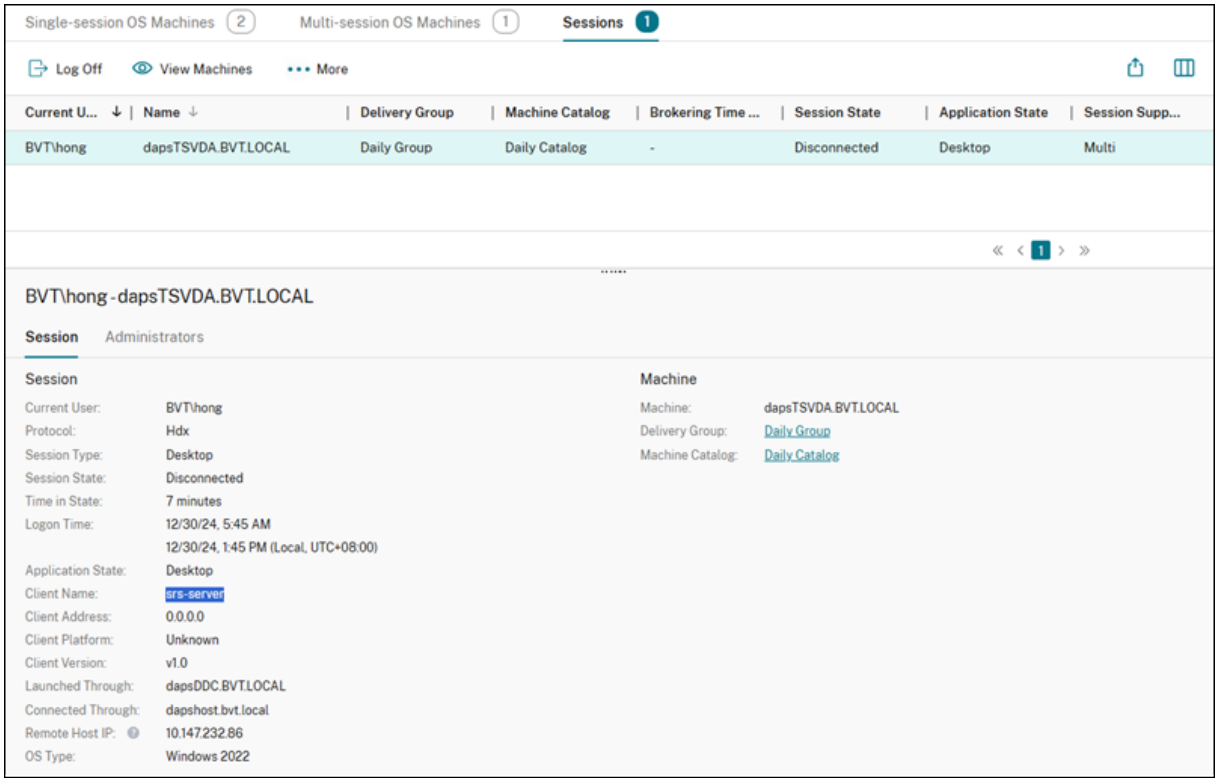


A prompt appears with a notification if the resource is launched successfully. Then, check the session in the studio.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



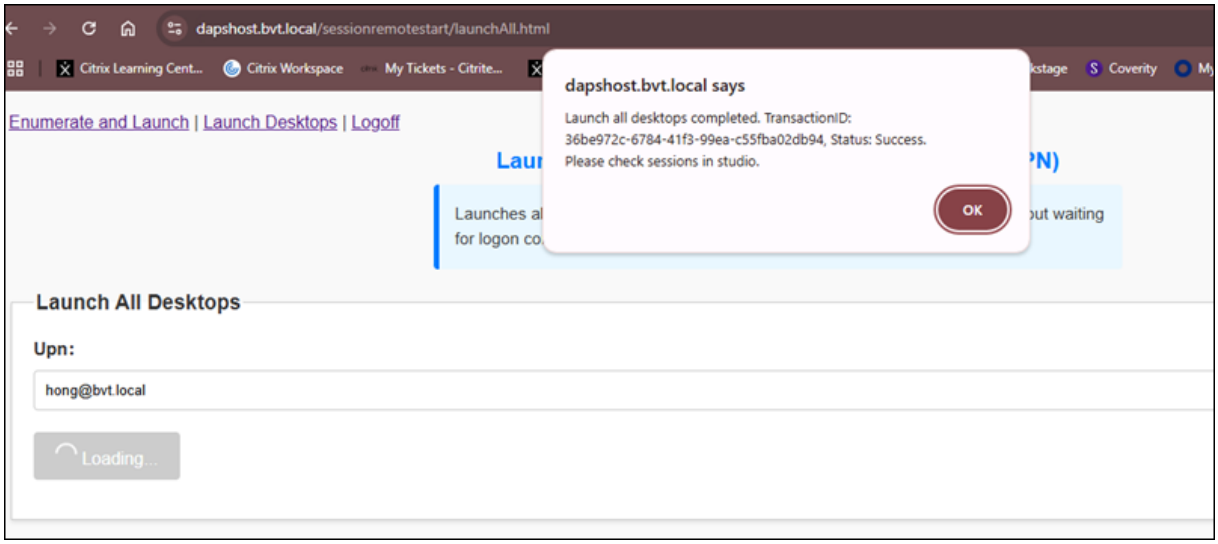
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



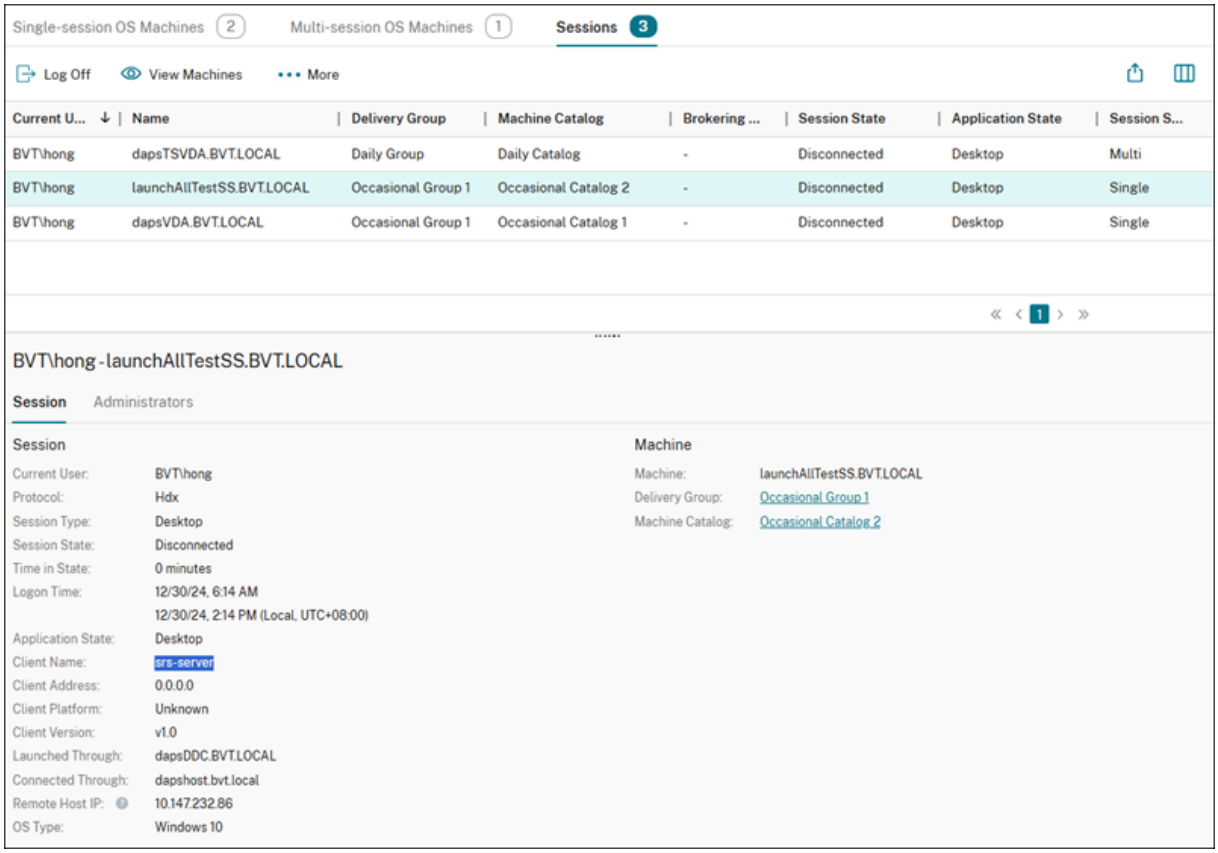
Launch Desktops

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.



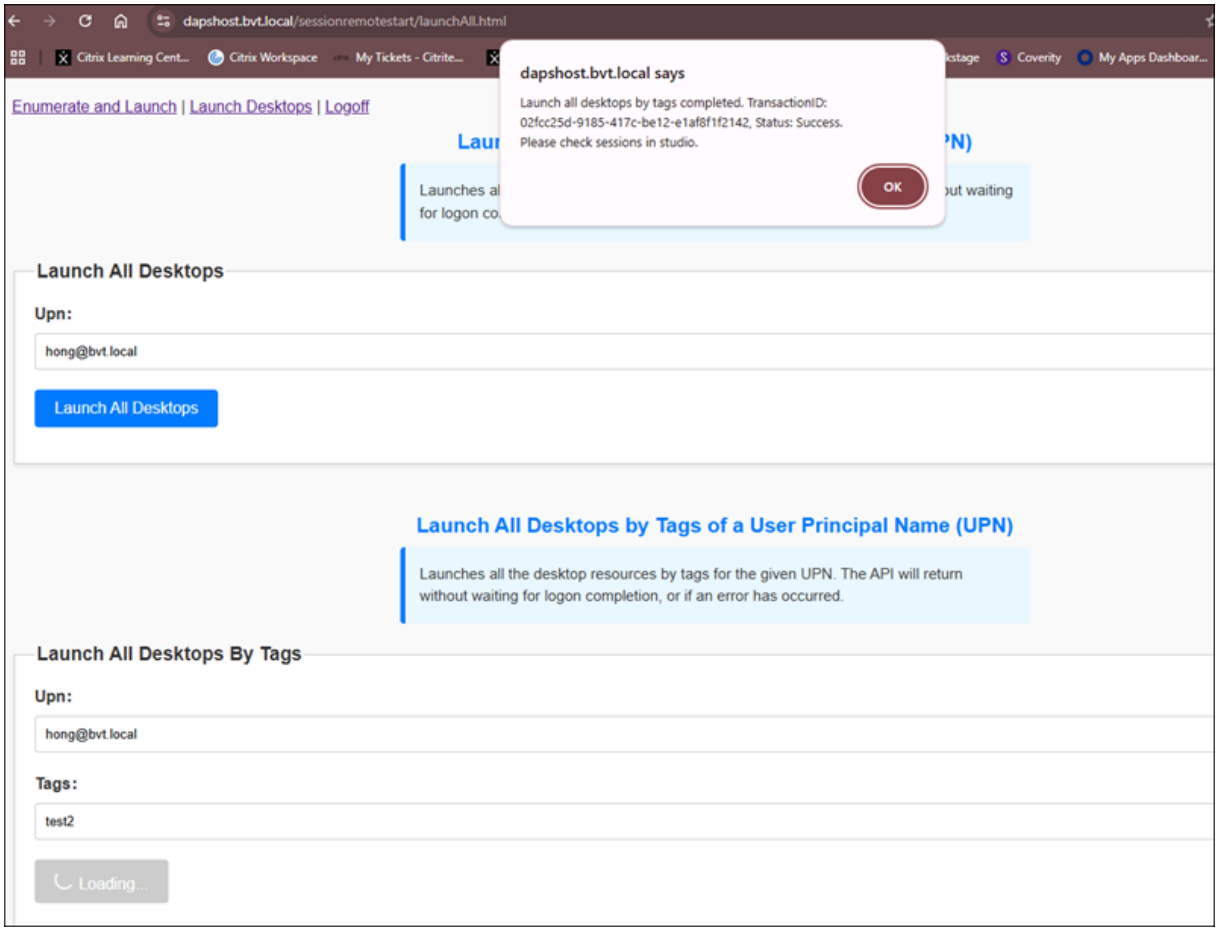
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



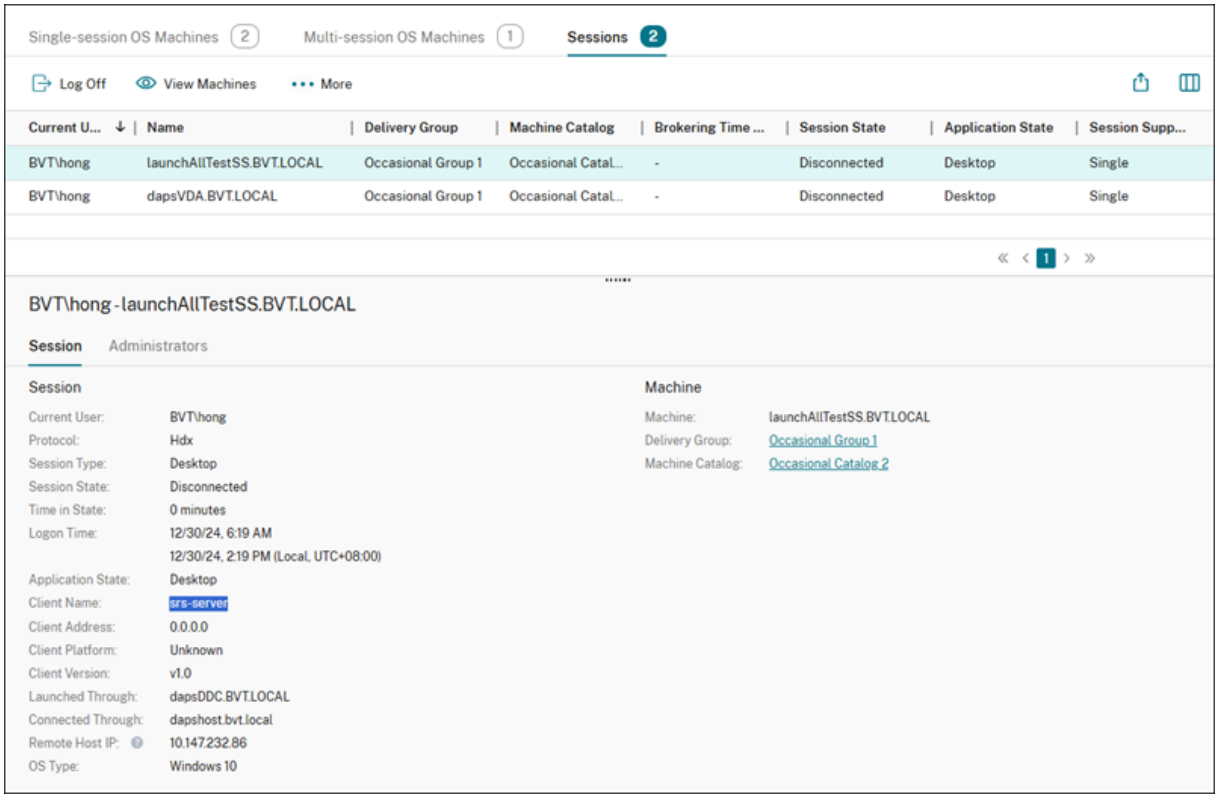
Launch All Desktops by Tags of a User Principal Name (UPN)

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



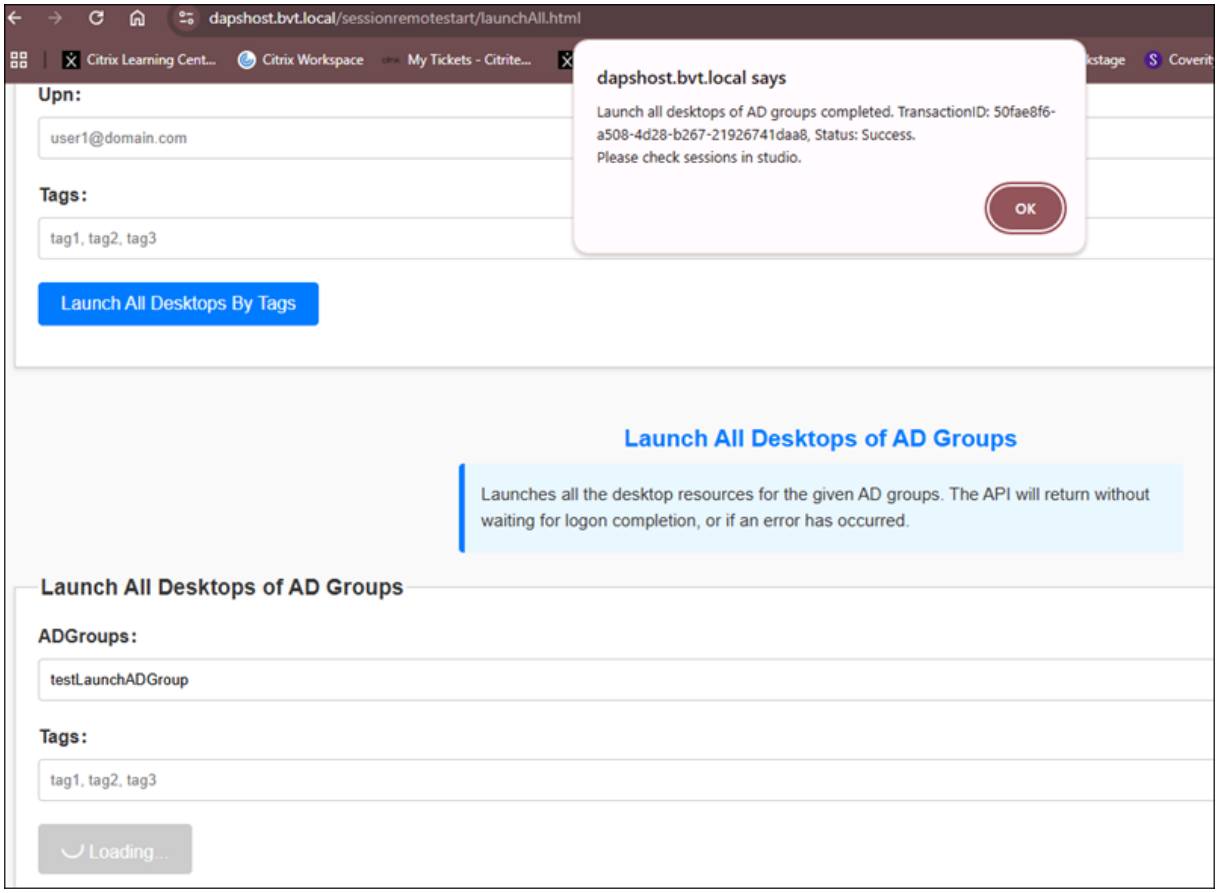
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



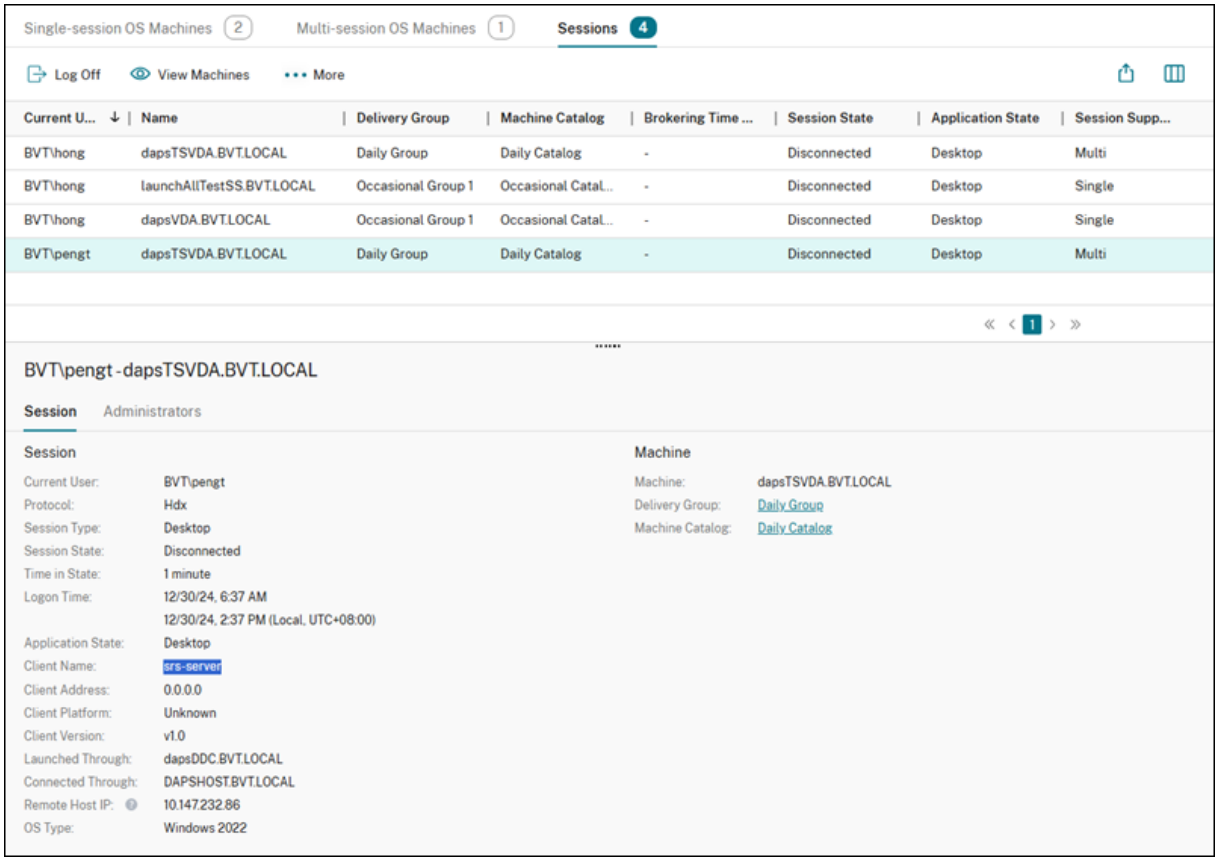
Launch All Desktops of AD Groups

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

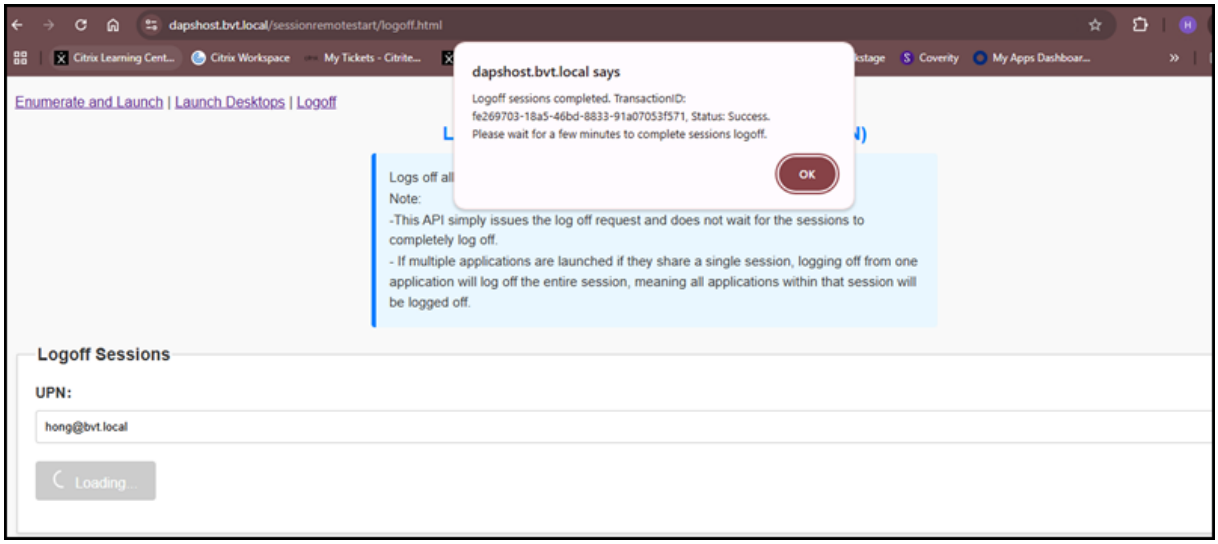


© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

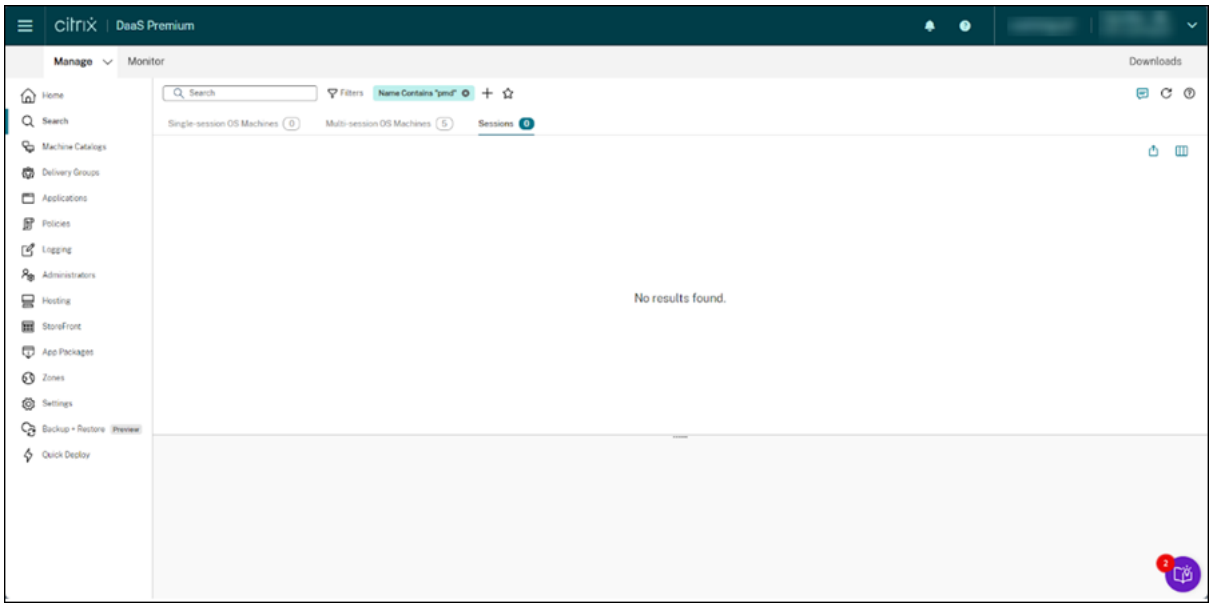
Output:

```
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 ----------------------------------------------
```

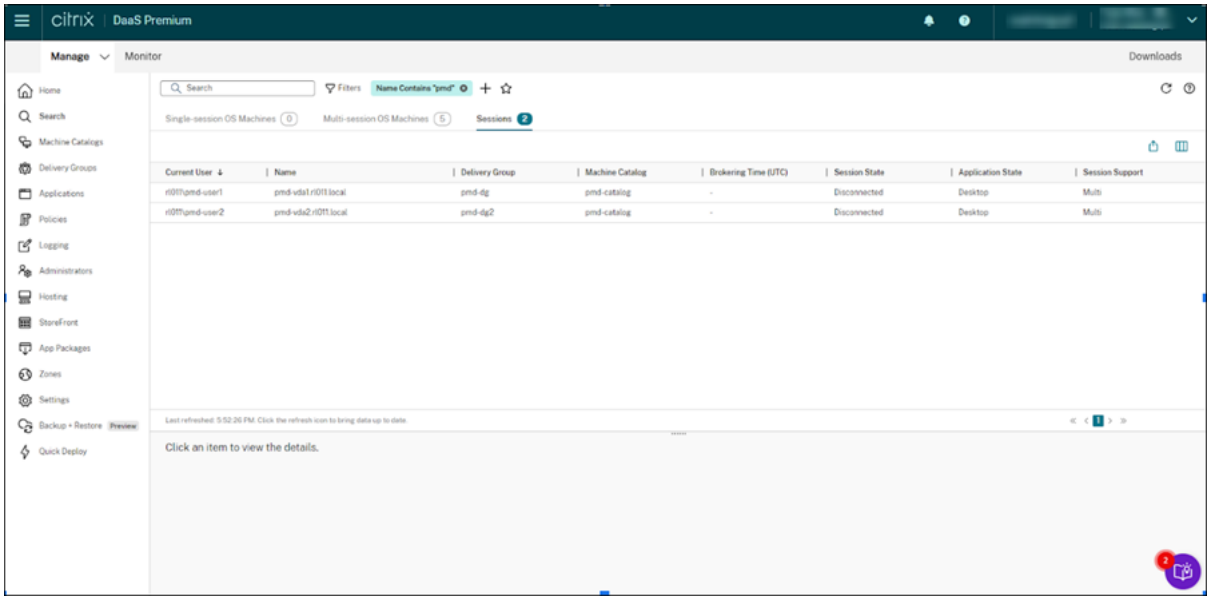
Verify the job output to make sure the resources are pre-launched successfully.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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



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.



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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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

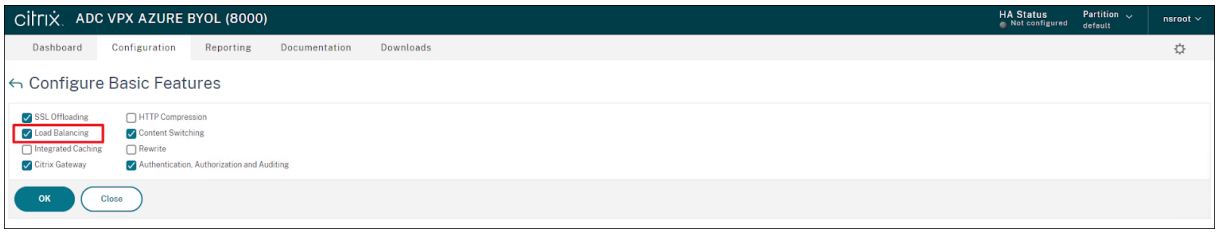
The following table lists the minimum requirements.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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**.



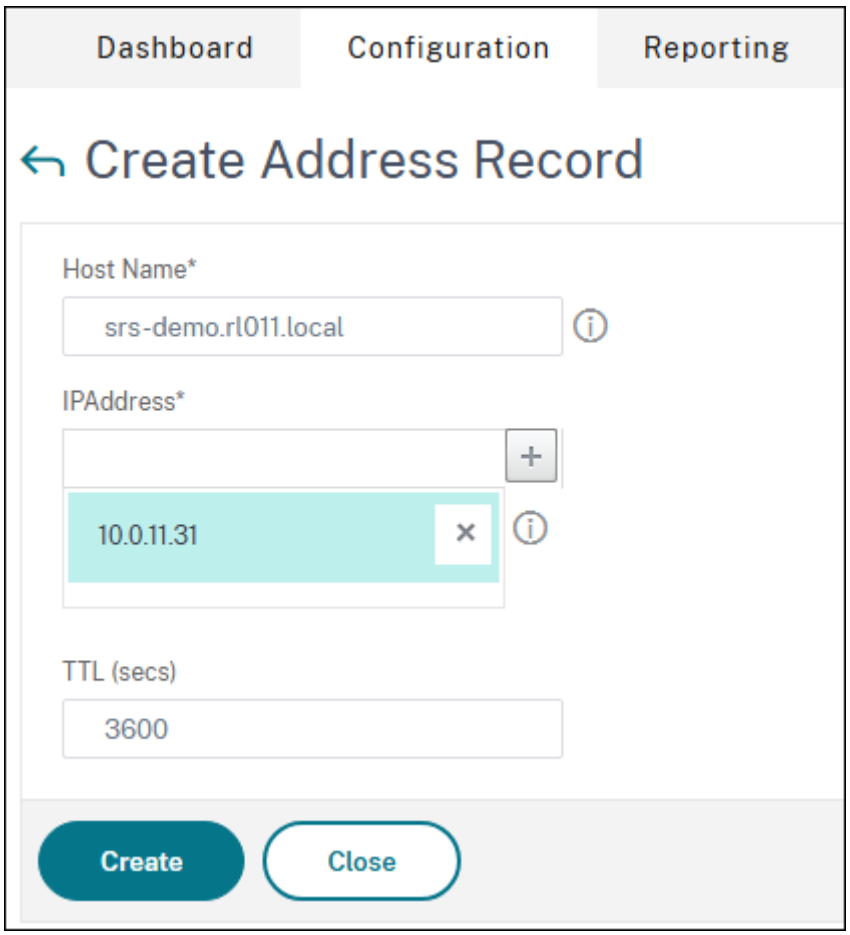
Configure server objects

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.

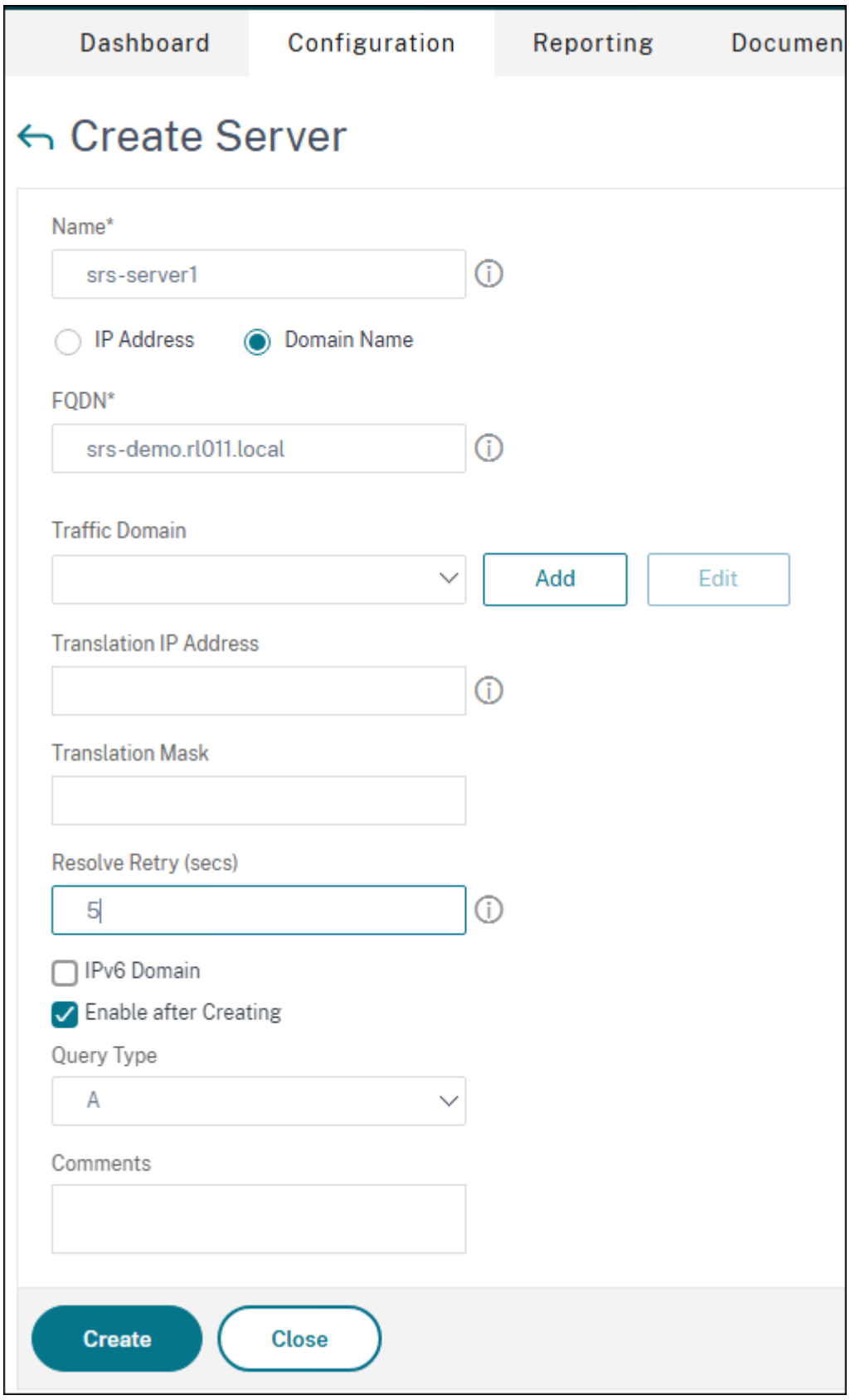
Navigate to **Traffic Management > DNS > Records > Address Records**, and add an address record.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

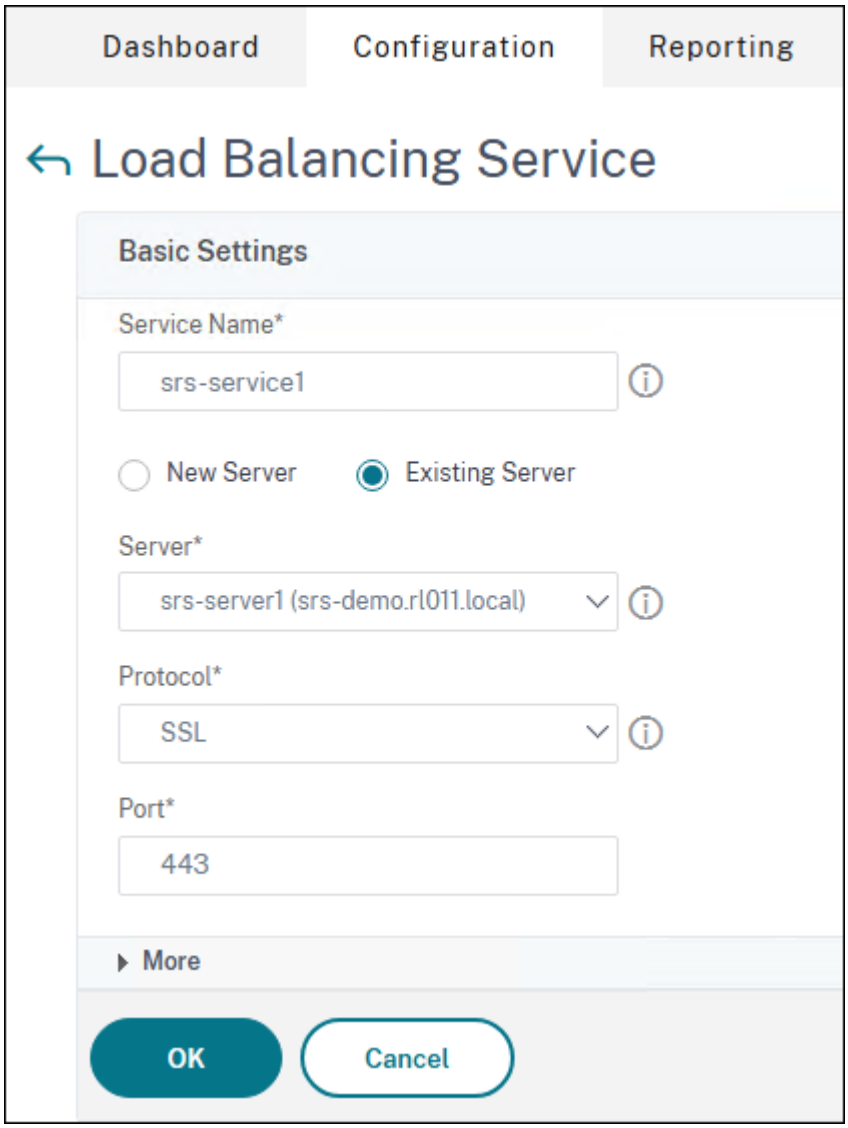


© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Repeat the two steps if you have multiple servers.

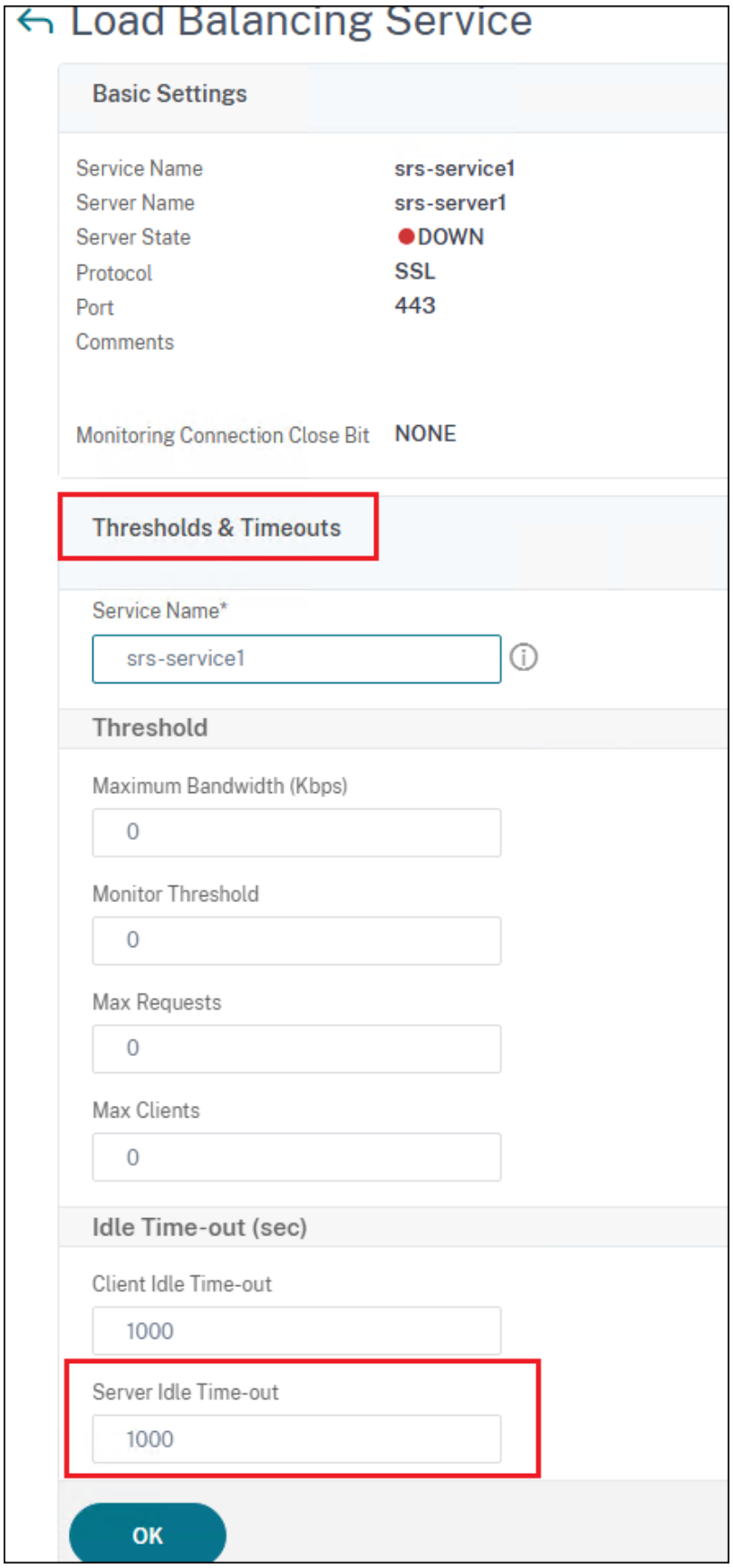
Configure services

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



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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

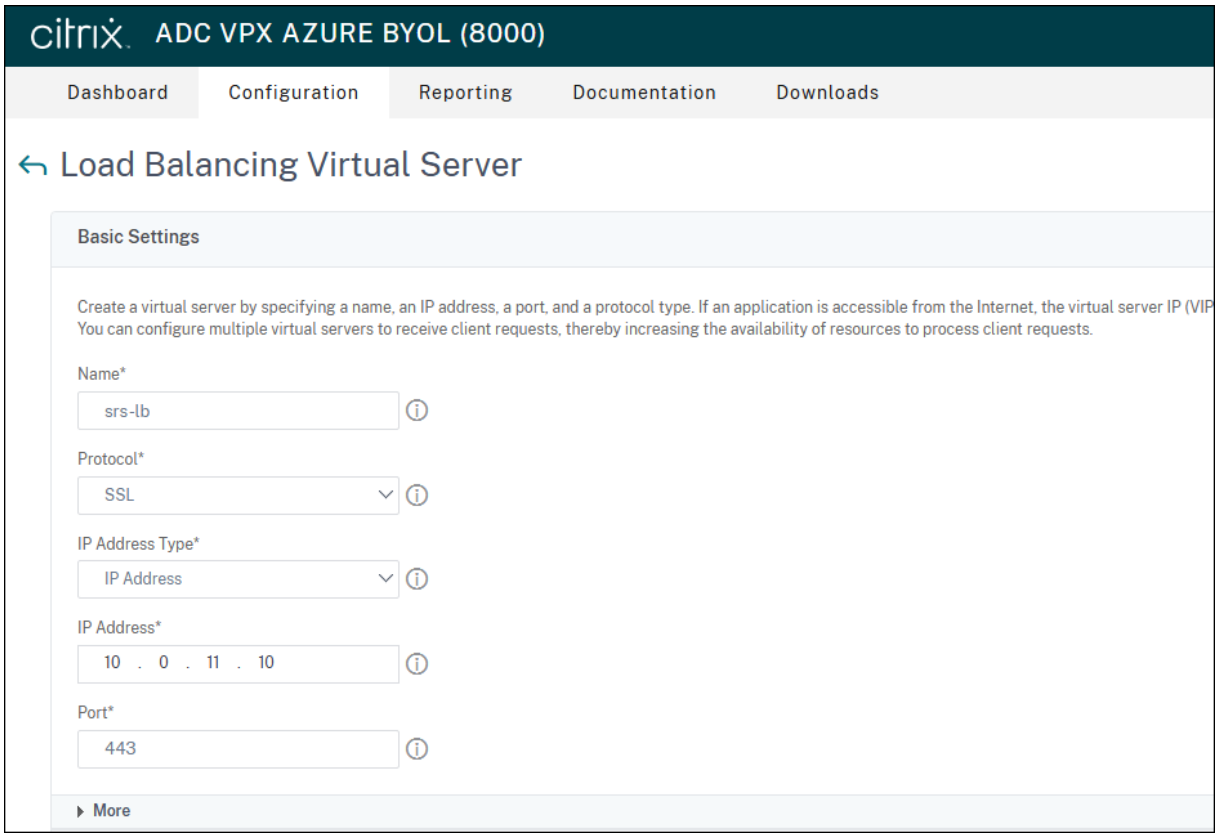


© 1999–2024 Cloud Software Group, Inc. All rights reserved.

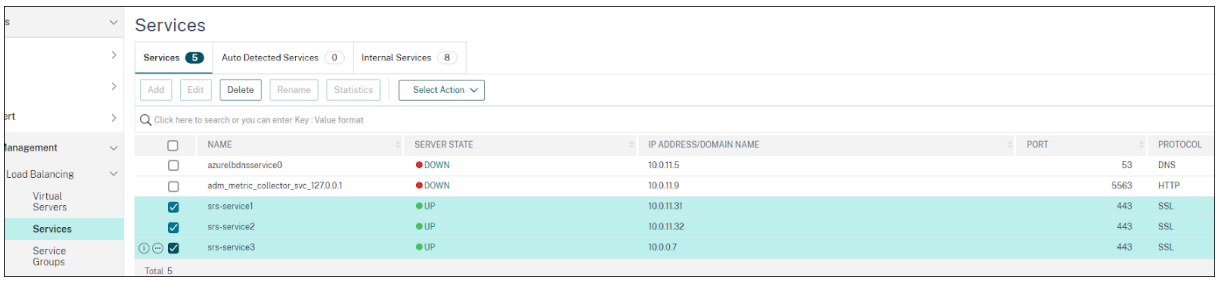
Repeat the operation if you have multiple servers.

Create a virtual server

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

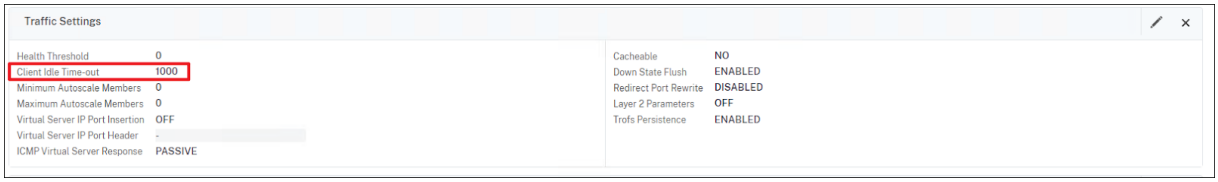


1. Bind services to the virtual server.



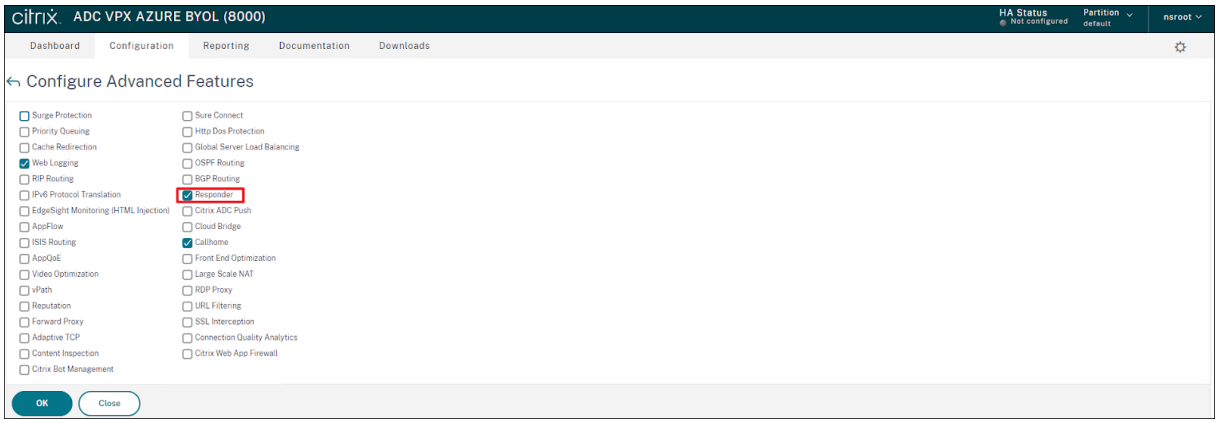
1. In **Traffic Settings**, modify the value of **Client Idle Time-out** according to the average launching processing seconds in your environment.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

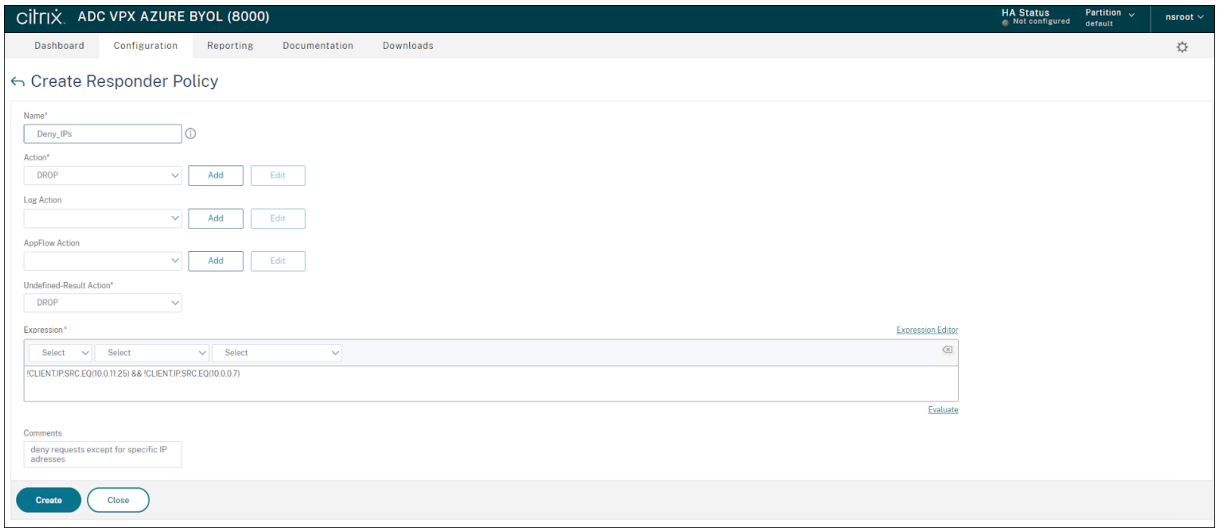


Configure a Responder Policy to drop untrusted IP addresses (Optional)

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



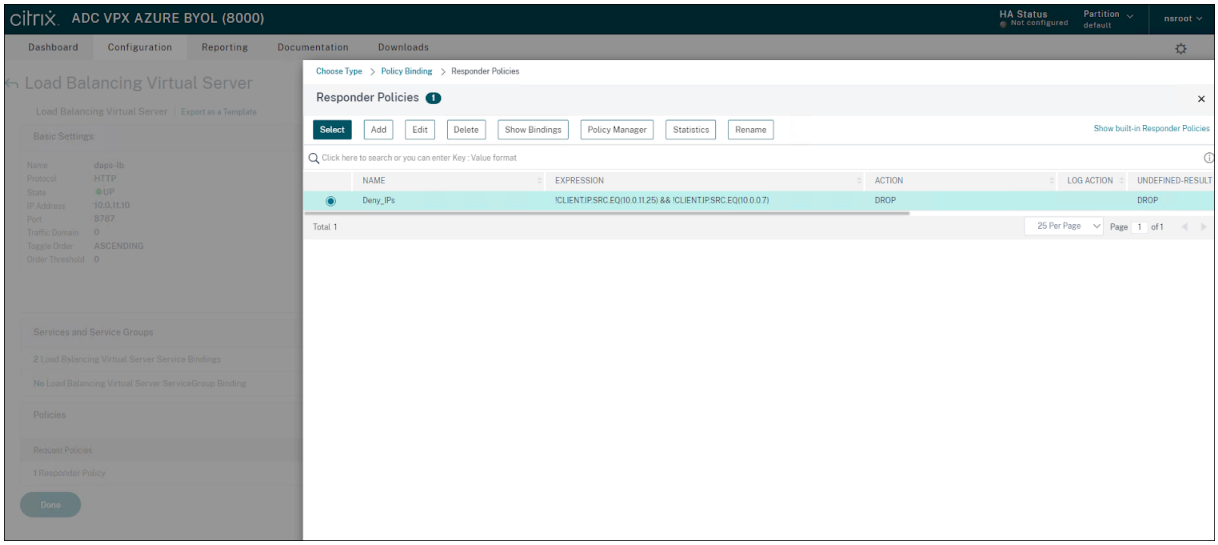
1. Configure a responder policy. Navigate to **AppExpert > Responder > Policies**, and add a policy.



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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

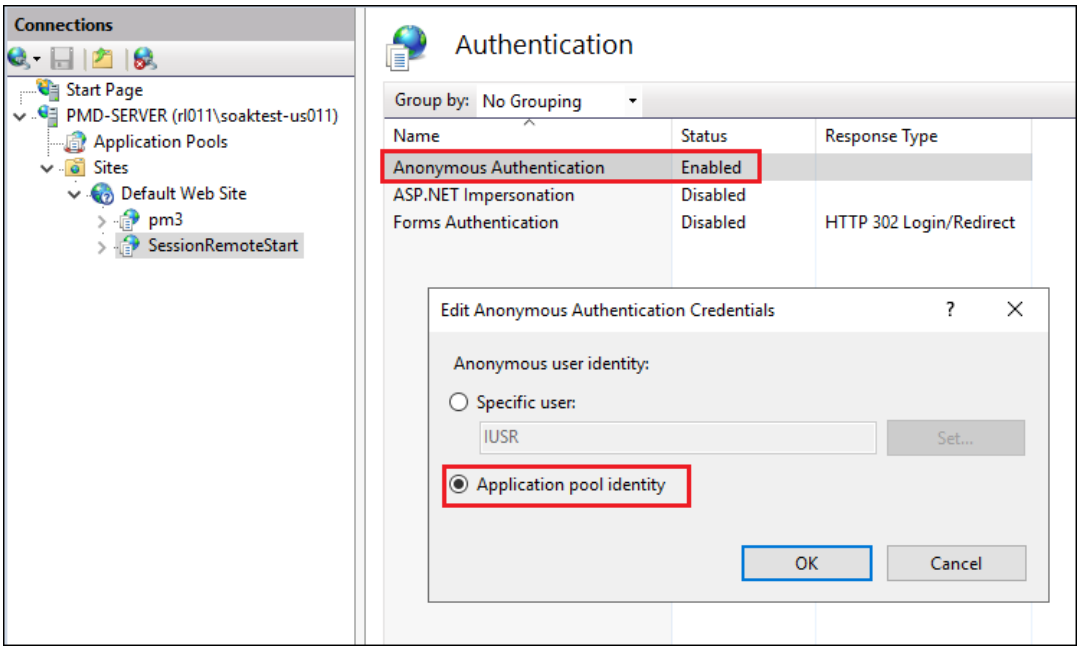
Log file permissions

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**.

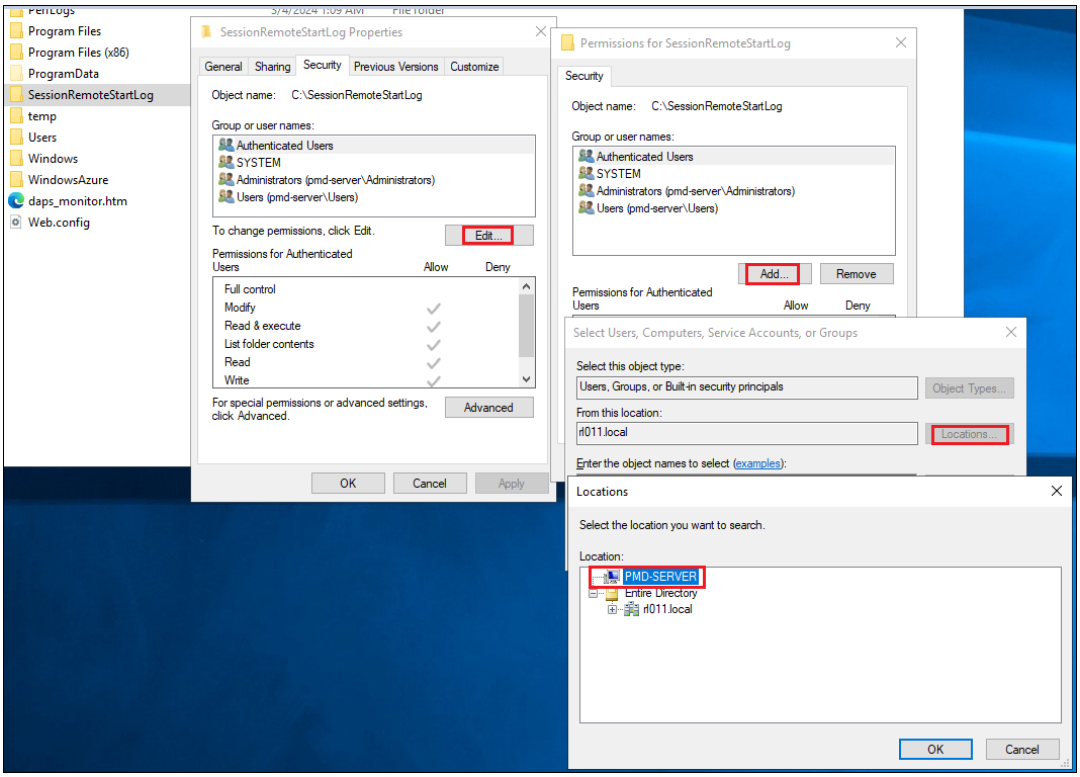
   b) Right-click **Anonymous Authentication** and select **Edit > Select Application pool identity**.



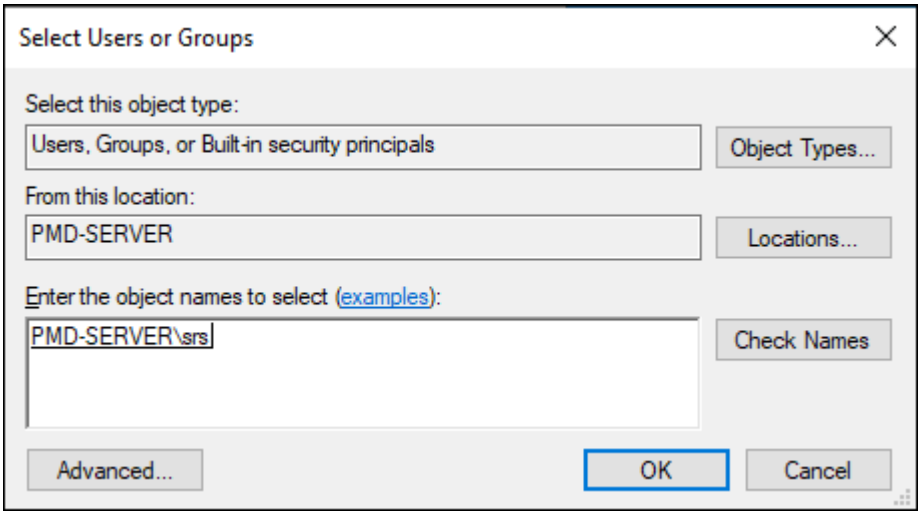
2. Now you can create a folder at your preferred location, and grant permissions to log to the new folder.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

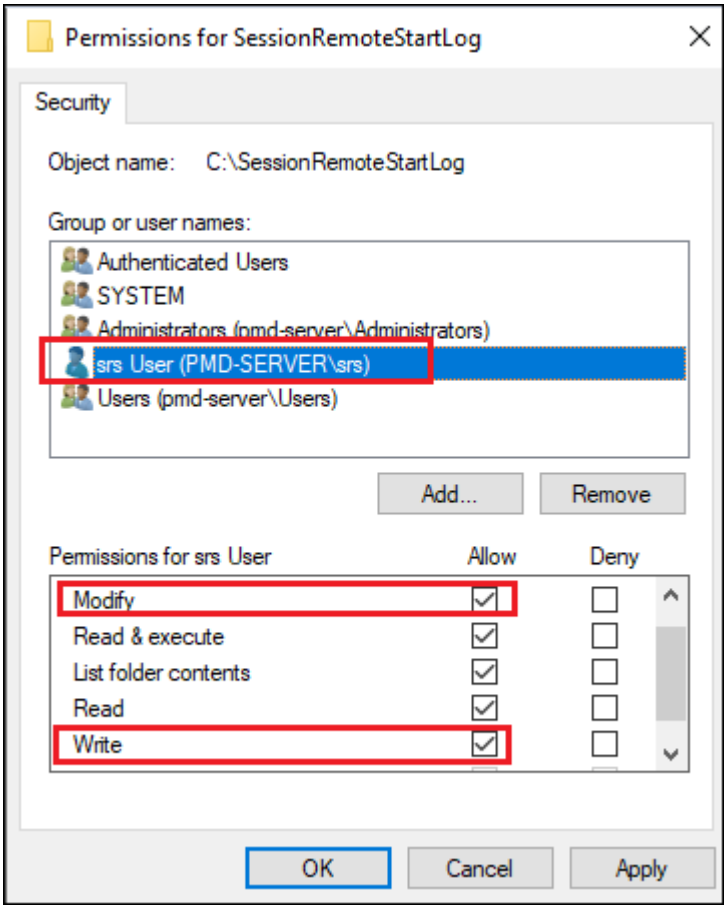


b) Input the Session Remote Start user created in the previous section. (If the default identity is used, input “IIS AppPool\SrsAppPool”instead).



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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



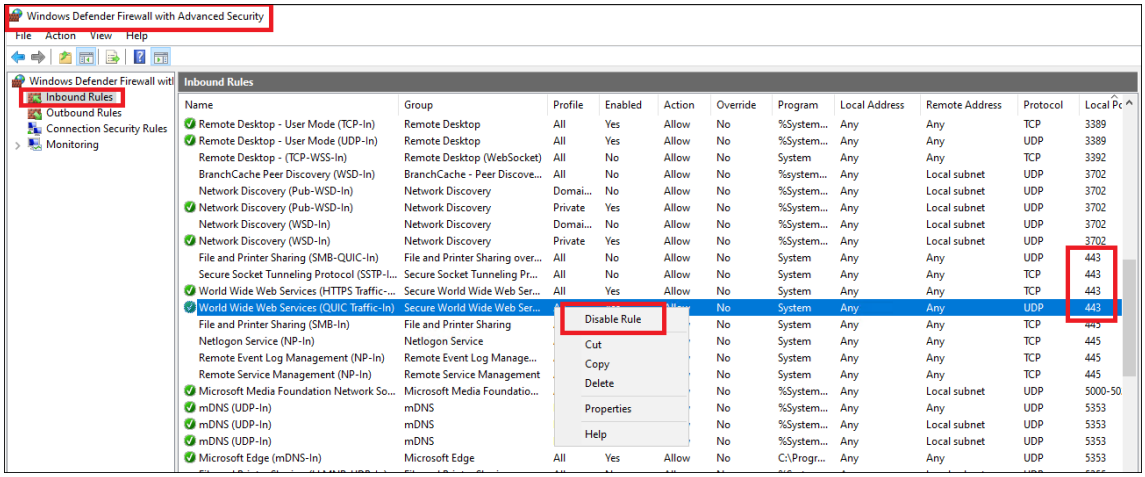
2. Configure Inbound Firewall Rules

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)**.

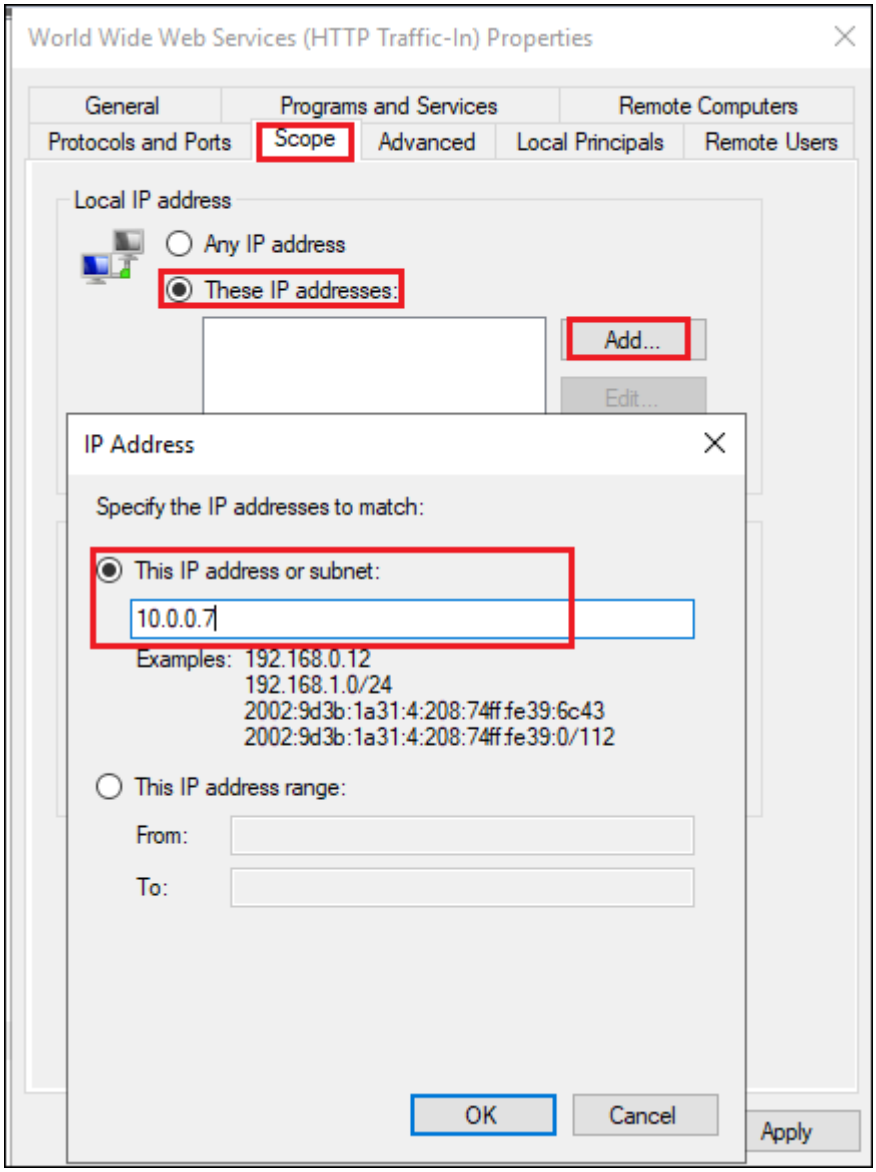
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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

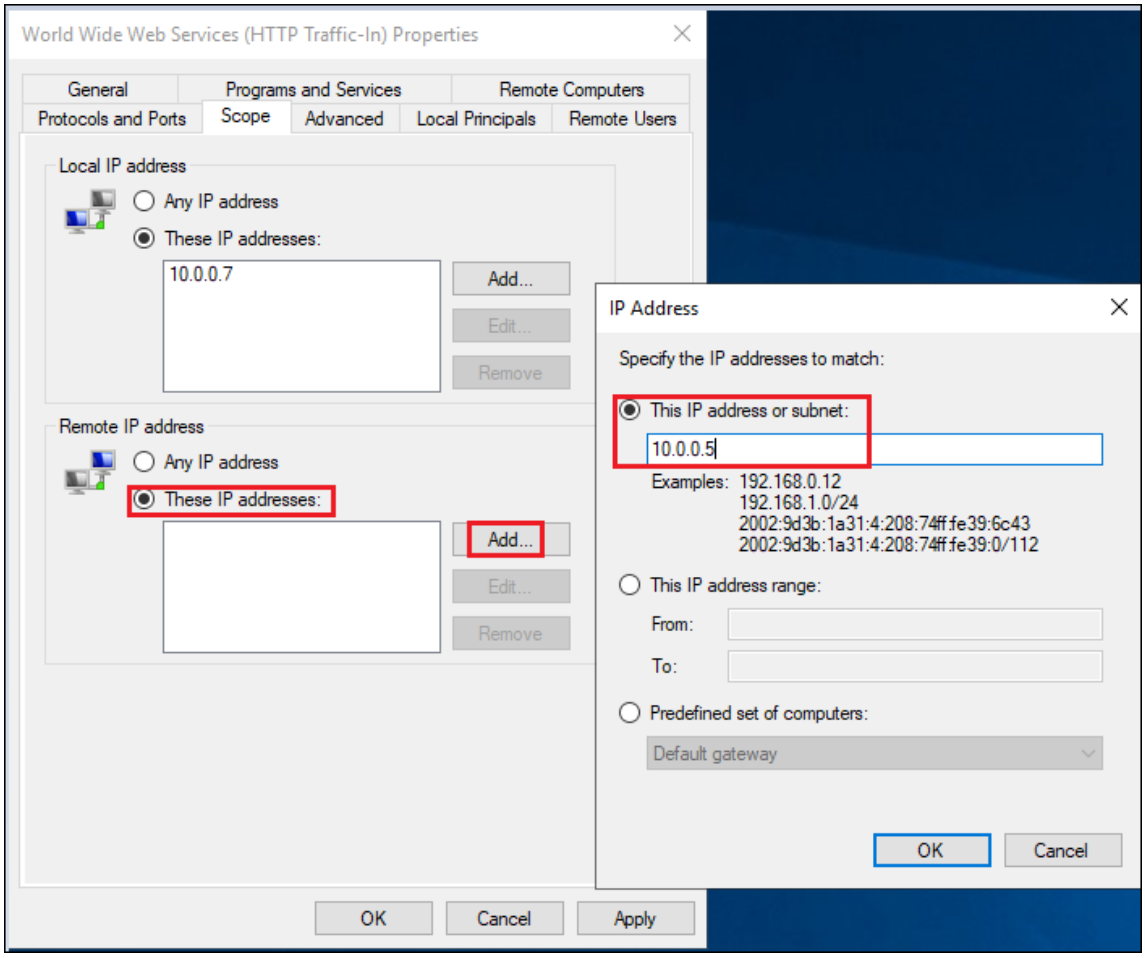
1. Double click ‘World Wide Web Service (HTTPS Traffic-In)’, open the ‘Properties’configuration, switch to ‘Scope’tab.
2. Add local IP address limitation. This is the local endpoint(s) (Network Interface) for 3rd-party Auth Service and StoreFront.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



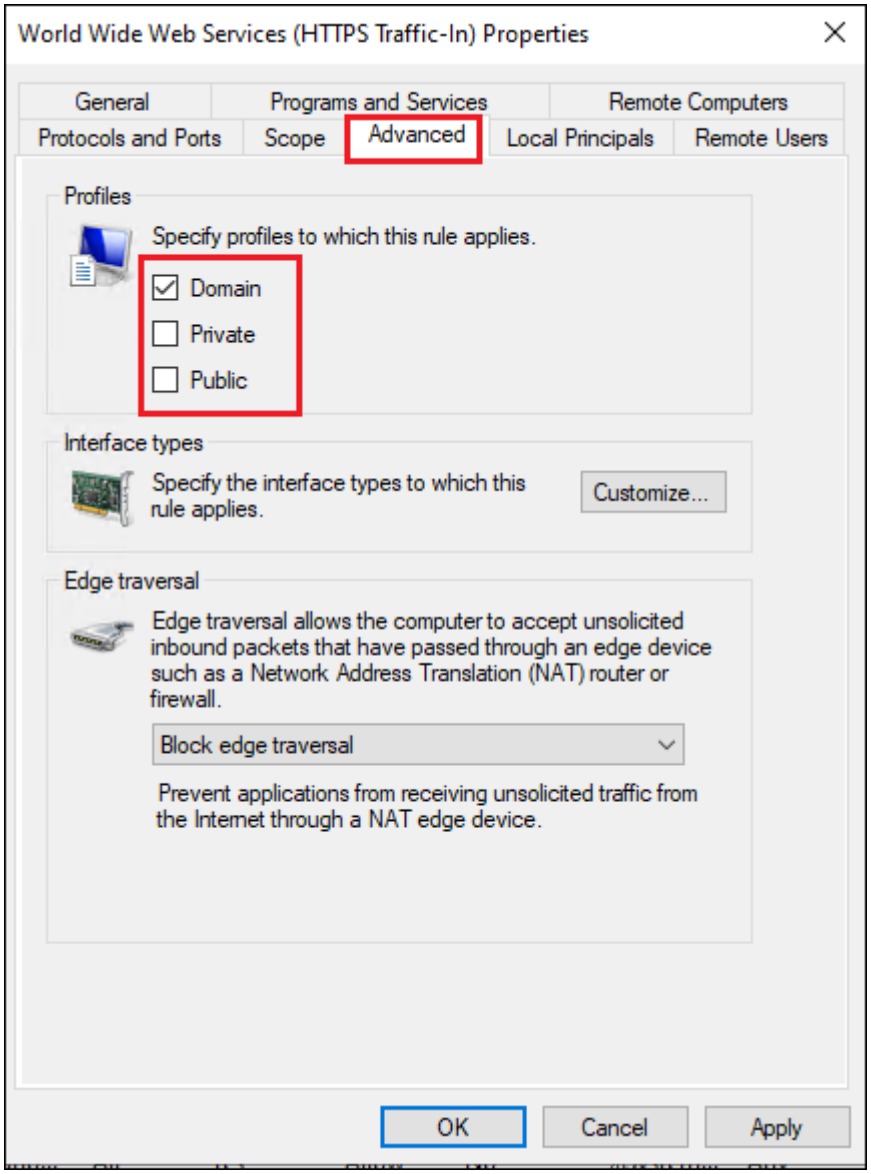
3. Add remote IP address limitation. Add IP addresses of 3rd-party Auth Service and StoreFront.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Third party firewall products will require configuring separately.

3. App Protection

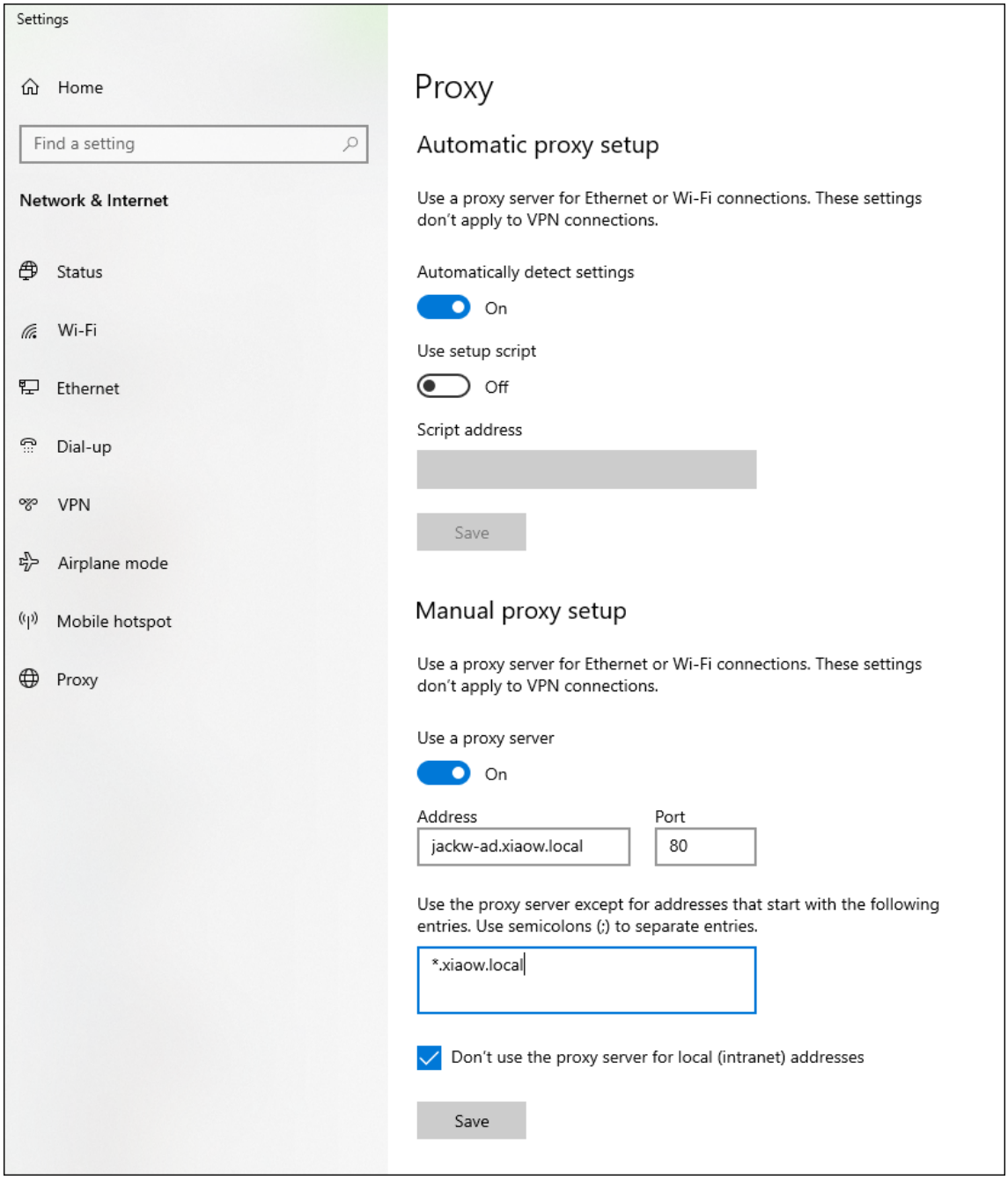
If App Protection is enabled for a delivery group, the customization described in this Citrix documentation must be applied to the Session Remote Start store:

4. HTTP Proxy Configuration

Session Remote Start supports only unauthenticated HTTP proxies.

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

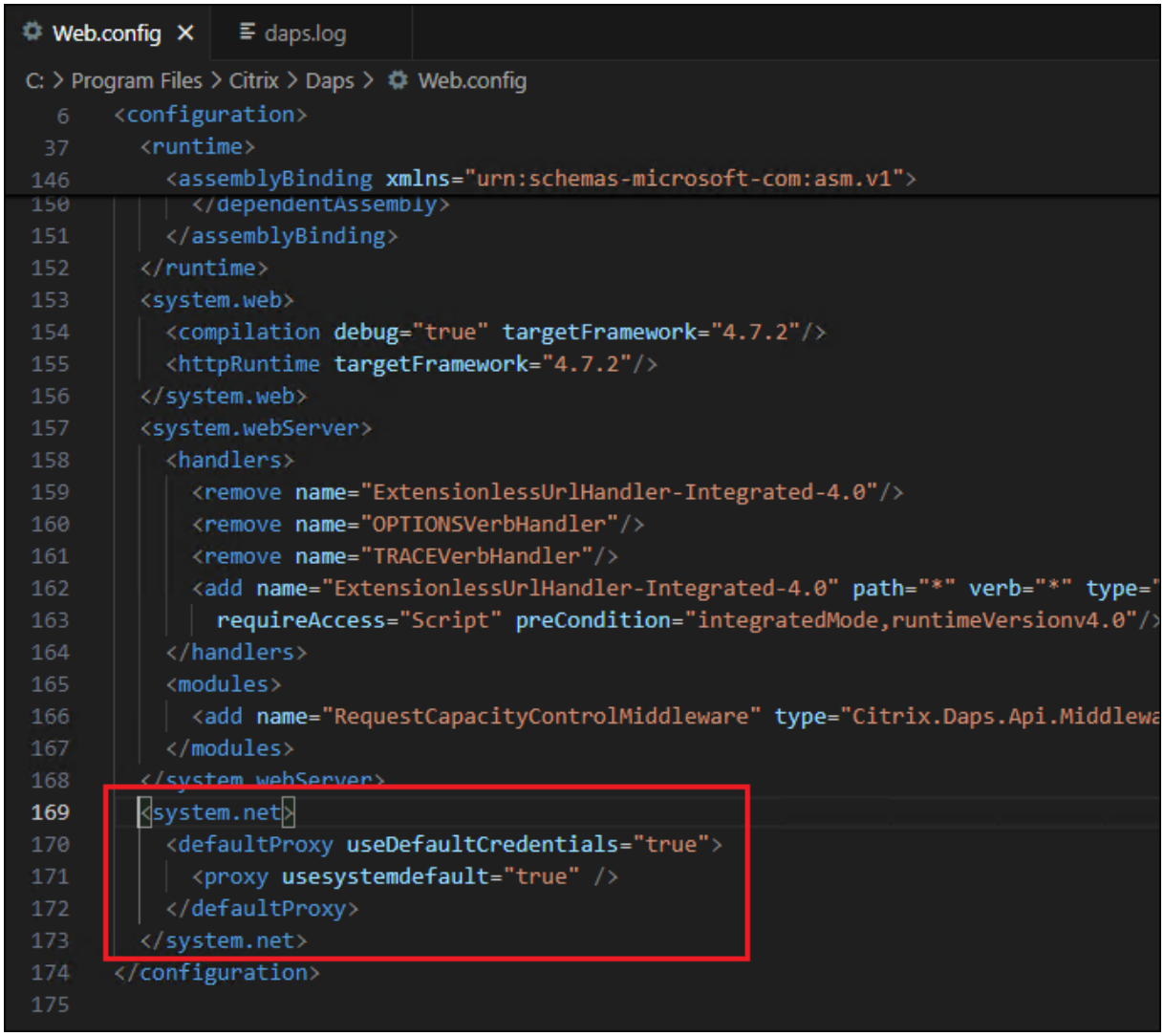
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

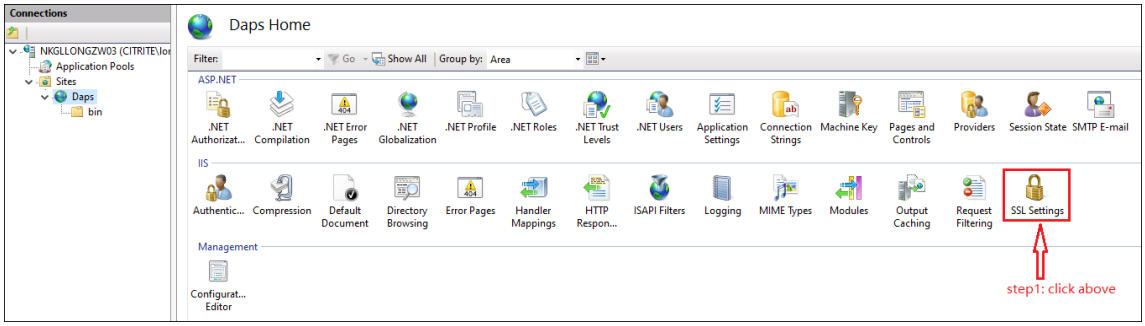


5. mTLS configuration

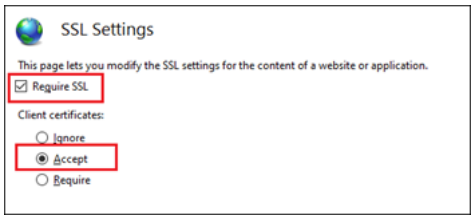
The Session Remote Start API does not require end-user authentication, unlike StoreFront. Therefore, it is crucial to ensure that only trusted services can communicate with the Session Remote Start Service. One method to achieve this is by enforcing mutual TLS (mTLS) authentication between the Session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

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

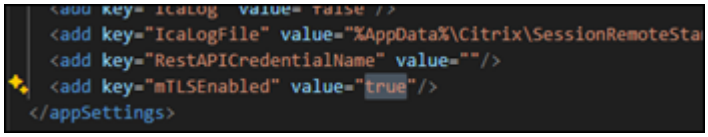
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



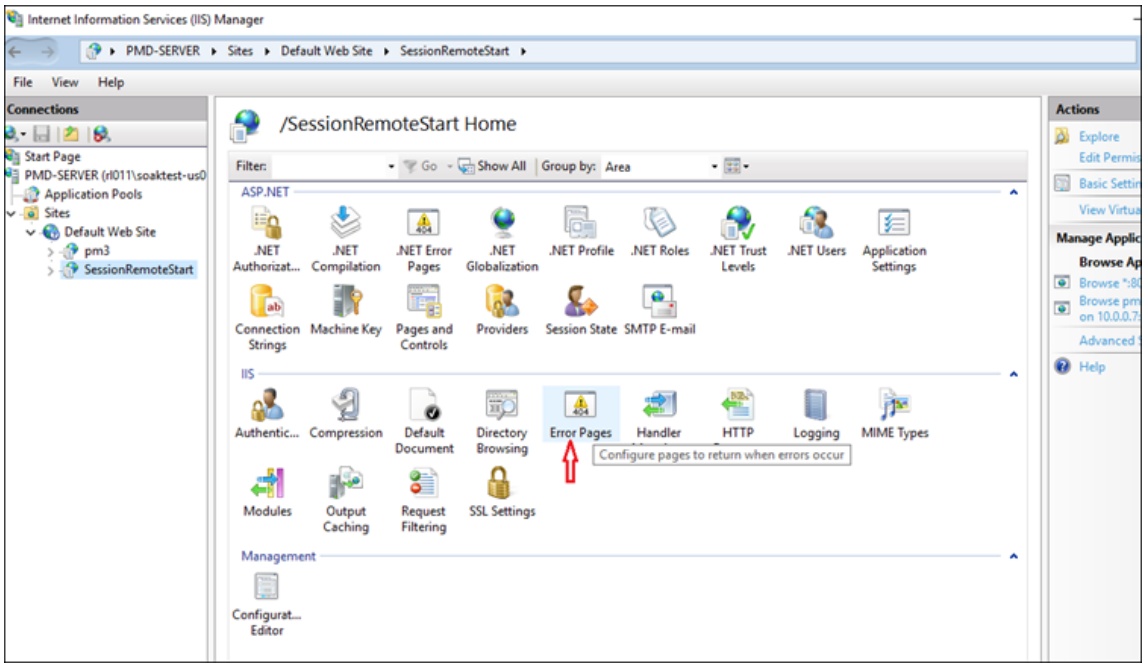
2. On the **SSL Settings** page, select the **Require SSL** and **Accept** check boxes and click **Apply**.



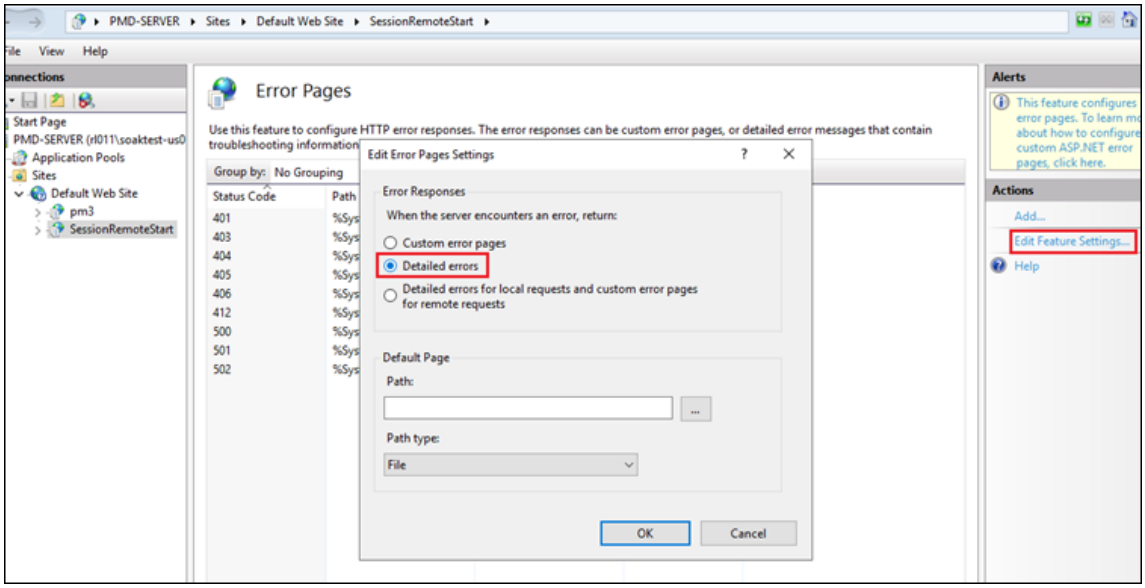
3. Edit the Web.config and change **mTLSEnabled** to `true`.



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



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

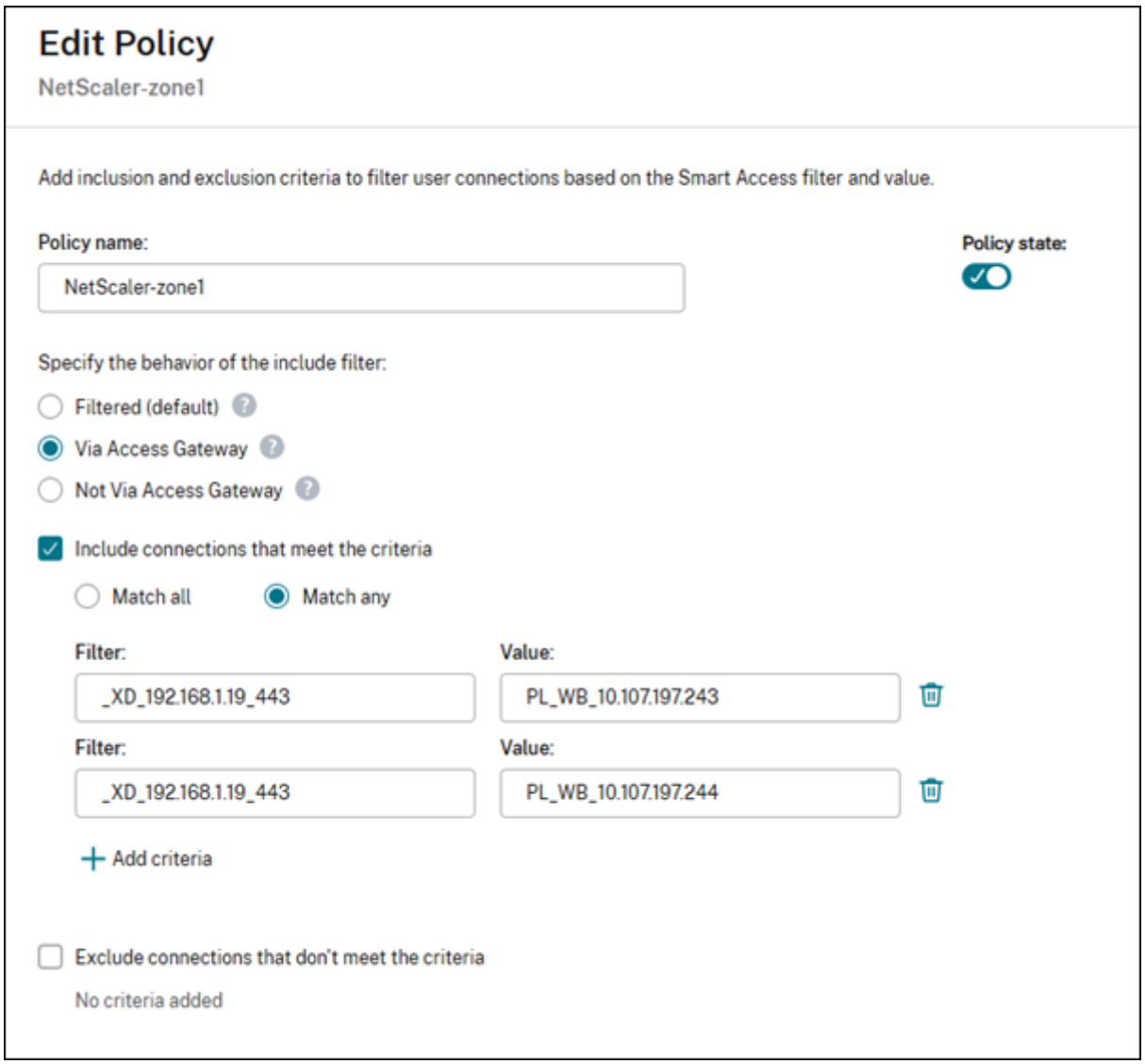


6. Filter enumerated resource results by Smart Access

We support the viaAG broker access rules.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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>
```

© 2024 Cloud Software Group, Inc. All rights reserved. This document is subject to U.S. and international copyright laws and treaties. No part of this document may be reproduced in any form without the written authorization of Cloud Software Group, Inc. This and other products of Cloud Software Group may be covered by registered patents. For details, please refer to the Virtual Patent Marking document located at https://www.cloud.com/legal. Citrix, the Citrix logo, NetScaler, and the NetScaler logo and other marks appearing herein are either registered trademarks or trademarks of Cloud Software Group, Inc. and/or its subsidiaries in the United States and/or other countries. Other marks are the property of their respective owner(s) and are mentioned for identification purposes only. Please refer to Cloud SG's Trademark Guidelines and Third Party Trademark Notices (https://www.cloud.com/legal) for more information.