Progress®
Kemp® LoadMaster®

Deployment Guide Citrix StoreFront for Virtual Apps and Desktops

Generated on: 16 September 2024

Copyright

Visit the following page online to see Progress Software Corporation's current Product Documentation Copyright Notice/Trademark Legend: Product Documentation Copyright Notice & Trademarks | Progress

Table of Contents

Chapter 1: Introduction 5

Chapter 2: Virtual Service Summary 7

Chapter 3: High-Level Flow (External) 9

Chapter 4: Requirements 11

Deployment Sizing Limitations 12

Chapter 5: Currently Unsupported Features 13

Chapter 6: Configure the LoadMaster 14

ESP 15

Configure using the Progress Kemp PowerShell Script 16

Installing a New Citrix Workload 16

Configure using the Progress Kemp Template 17

Template 18

Global Settings 18

Import the Template 19

Citrix StoreFront Internal Configuration 19

Create and Update the Virtual Services and Secure Listeners (External) 20

Secure Listeners 24

Modify the Content Rules 26
SSL Certificate 29

Chapter 7: Citrix StoreFront Settings 31
Configure HTTP Basic Authentication 32
Configure WebSocket Policy 33

Chapter 8: Testing 34
Testing Workspace Receiver Application 34
Testing HTML5 Web Socket Connection 35
Troubleshooting 35

Chapter 9: Appendix 36

1

Introduction

Introduction

Citrix Virtual Apps and Desktops provides virtualization solutions that give IT control of virtual machines, applications, and security while providing anywhere access for any device through Citrix StoreFront service. End-users can use applications and desktops independently of the client device's operating system and interface.

A key factor in delivering Virtual Apps and Desktops is ensuring the resilience, performance, and scalability of the Virtual Desktop Infrastructure (VDI) with duplication of VDI servers and services. Load balancers are an essential component of this infrastructure as they provide a central connection point for remote users, can detect infrastructure outages, offload encryption overhead, and provide additional layers of security.

In contrast to Citrix ADC (NetScaler) load balancing that is often the default choice for StoreFront services, the LoadMaster is easy to configure, offers significant cost of ownership savings, and is supported by a world-class technical team.

LoadMaster is a drop-in load balancer replacement for Citrix ADC (NetScaler) that includes pre-defined templates for common Citrix Virtual Apps and Desktops environments to greatly simplify deployment and ensure optimal security and performance. LoadMaster offers significant Total Cost of Ownership (TCO) savings compared to Citrix ADC and is supported a technical team that regularly achieves 99% customer satisfaction ratings.

A Virtual Service template, PowerShell script, and this deployment guide was introduced with LoadMaster Operating System (LMOS) 7.2.51 to deploy a Virtual Service as a Citrix StoreFront Gateway for external publishing of Citrix Virtual Apps and Desktops deployments, so that internet clients can leverage Citrix's VDI. In previous releases, the LoadMaster only supported publishing to internal networks.

The Progress Kemp-approved and tested template supports authentication of clients to a Citrix StoreFront endpoint that provides access to Citrix Virtual Apps and Desktops resources. Clients can log in using Citrix Workspace App, Citrix Receiver, or a browser such as Edge, Chrome, Firefox, or Safari.

2

Virtual Service Summary

Virtual Service Summary

Here is a summary of the Virtual Services:

- **StoreFront Gateway:** This Virtual Service is the main endpoint and will identify whether the client is connecting using Citrix Workspace/Receiver or using a browser. This Virtual Service IP address will be configured for your external DNS record, for example **citrix.domain.com** which will NAT to your Virtual IP address. Depending on the template selected, the StoreFront Gateway Virtual Service consists of several Sub Virtual Services:
  - **StoreFront Browser Auth ESP:** Handles front-end authentication using the Edge Security Pack (ESP) for protocols such as RADIUS and LDAP.
  - **StoreFront Browser Launch HTML5 App:** Handles the rewriting of the ICA file where a HTML5 WebSocket connection had been detected.
  - **StoreFront Workspace-Receiver Pass Through:** Handles pre-requests for Workspace/Receiver ESP front-end authentication.
  - **StoreFront Workspace-Receiver Launch App:** Handles the rewriting of the ICA file where the Citrix Workspace/Receiver application has been detected.
  - **StoreFront Workspace-Receiver Auth ESP:** Handles front-end authentication for Workspace/Receiver.
- **Secure Listeners:** The **Citrix StoreFront Gateway** template also creates ten (10) individual Secure Listeners which will listen on a secure port such as port 4431 and forward the connection to your VDI server on port 2598. The **Citrix StoreFront Gateway - HTML5** template also creates ten (10) Secure Listeners, five (5) Secure Listeners to handle native ICA 2598 traffic, and five (5) Secure Listeners to handle HTML5 web socket 8008 traffic. These listeners correspond to specific internal VDI servers. This is explained in the Secure Listeners section of this document.

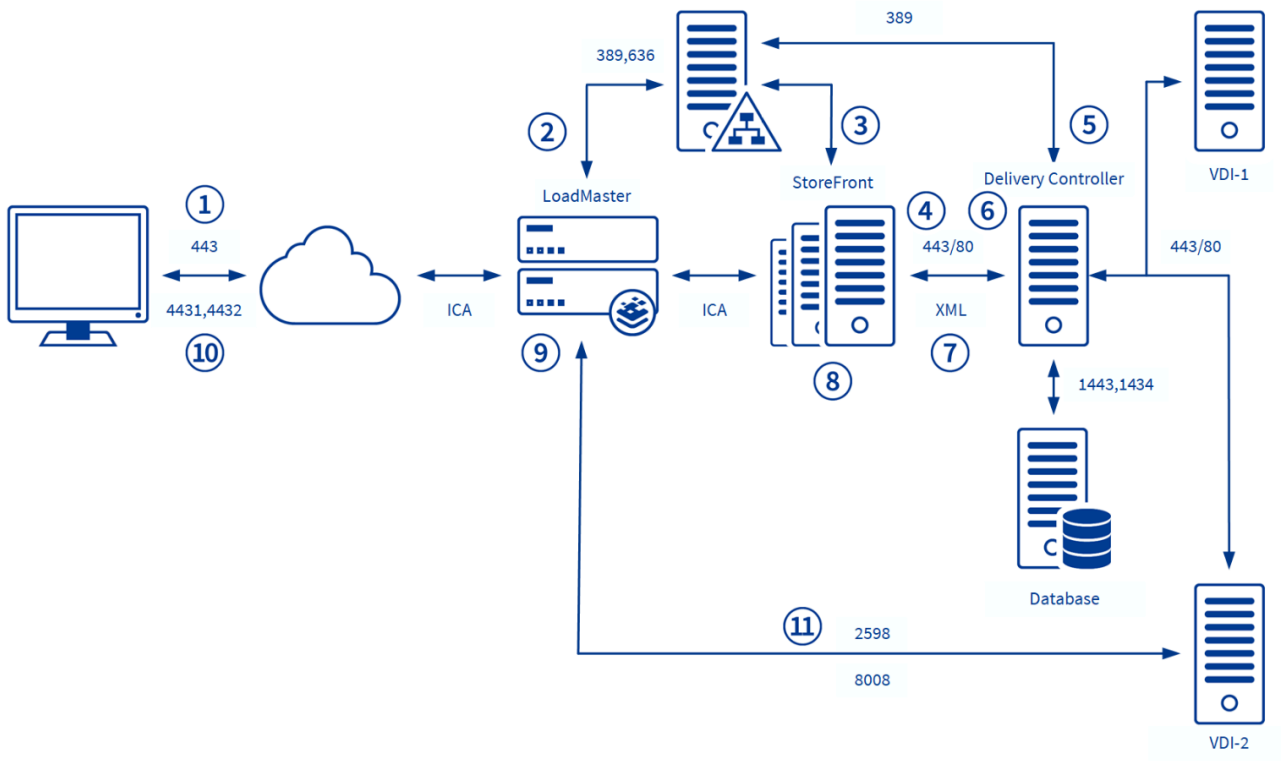
- **Content Rules:** The template creates several content rules with the name starting **Citrix_** to support the Virtual Services and Secure Listeners. No content rules are created by the **Citrix StoreFront Internal** template.
- **Citrix StoreFront Internal:** This Virtual Service is used to handle internal StoreFront connections. When a client launches an application through StoreFront the client connection is forwarded directly to the server.

3

High-Level Flow (External)

High-Level Flow (External)

In a Citrix Virtual Apps and Desktops environment, the LoadMaster sits at the edge (behind a firewall) and accepts connections from remote clients, load balancing connections across the available StoreFront servers. The LoadMaster manages the authentication to the external authentication systems such as Active Directory or RADIUS. When StoreFront returns the ICA file to the client, LoadMaster intercepts and modifies the information with the appropriate load balanced VDI server information.



The high-level flow is as follows:

1. The client connects to StoreFront using the LoadMaster.
2. The LoadMaster authenticates the client against Active Directory (AD) and assigns an "LMData" authentication cookie.
3. The LoadMaster POSTs credentials to StoreFront where StoreFront authenticates against AD.
4. StoreFront forwards credentials to the Delivery Controller in an XML query.
5. The Delivery Controller enumerates the user's applications by querying Active Directory for the Users Security Groups and queries the database for a list of the client's applications.
6. The client selects their application where StoreFront queries the Delivery Controller to find a suitable VDI server which contains the application.
7. The Delivery Controller returns the application information back to StoreFront in an XML file.
8. StoreFront creates an ICA file with the connection details such as the IP address of the VDI server and a launch reference.
9. The LoadMaster consumes the ICA file and rewrites the settings which enables the client to make a secure, publicly resolvable connection.
10. The LoadMaster forwards the ICA file to the client where the client automatically initiates a new connection over a secure port such as port 4431.
11. The LoadMaster receives the encrypted connection, decrypts, and forwards to the chosen VDI server.

4

Requirements

Requirements

The following requirements must be met:

- For ESP pre-authentication you will require an onsite authentication server such as a RADIUS, LDAP, or SAML IDP server.
- You must have a LoadMaster Enterprise/Enterprise Plus subscription (or a trial license).
- You must use the Progress Kemp PowerShell script (preferred) or Citrix StoreFront Virtual Apps and Desktops template to configure your LoadMaster.
- You must have a Certificate Authority (CA) certificate to decrypt the SSL traffic for external connections.
- You must have external firewall rules configured for ports 443 and 4431- 4440. This port range accommodates 10 VDA/VDI servers. For Virtual Desktop environments, a larger port range is required to be open.
- LoadMaster firmware version 7.2.53 or above is required.
- Adding a StoreFront account to Workspace/Receiver requires both the internal and external Store URL to be the same.
- For an environment that contains up to 100 VDA servers, 4GB of memory is sufficient. For environments where there is up to 250 VDA servers, 8GB is required. For environments of up to 500 VDA servers, 16GB of memory is required.

Related Links

- Deployment Sizing Limitations

Deployment Sizing Limitations

Deployment Sizing Limitations

This solution can accommodate an organization with up to 500 VDA Servers.

5

Currently Unsupported Features

Currently Unsupported Features

In this implementation of Citrix StoreFront support, several features are currently unsupported:

- Front-end authentication (ESP) to StoreFront using Smart Cards (client certificates) is not supported.
- The LoadMaster currently supports TCP ICA/HDX with Session Reliability. UDP ICA/HDX with Session Reliability is not supported.Step 1: Disable HDX
- ICA file signing – which is not enabled by default in StoreFront – is not supported.
- Multitenancy is not supported.

6

Configure the LoadMaster

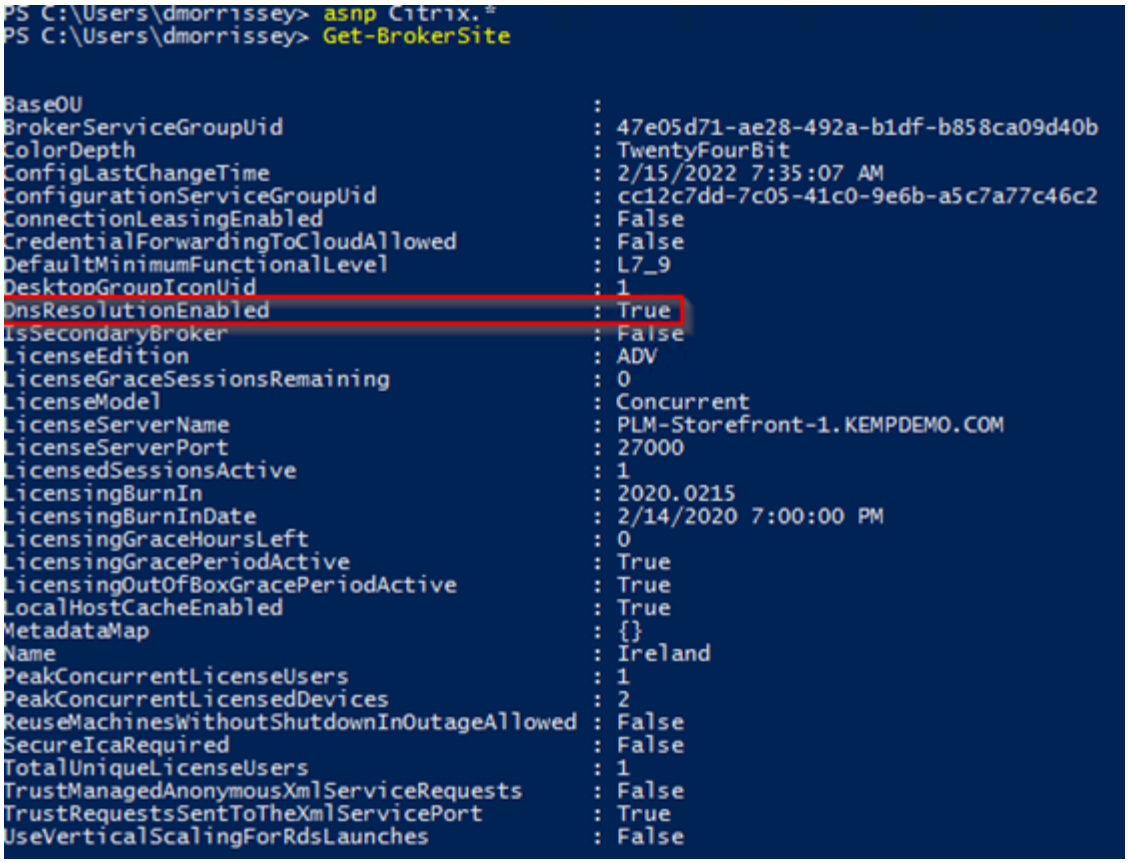
Configure the LoadMaster

To configure the settings on your LoadMaster, you can either use the Progress Kemp PowerShell script that is included in the Zip file, or the Progress Kemp template. We recommend using the PowerShell script because it removes the process of manually configuring your internal VDI server content rules, while also removing a lot of the repetitive steps relating to your Citrix StoreFront Store name. Refer to the relevant section below depending on whether you choose to use the PowerShell script or the template.

Note: The template is only recommended when testing with no more than ten (10) VDA/VDI servers. When configuring the production Virtual Desktops environment, you must configure it using the easy-to-follow PowerShell script.

Note: Ensure to take a LoadMaster backup before configuring so that you can restore if needed (for example, if the Citrix configuration is not successful). Restore the backup before attempting to configure for a second time using the template or PowerShell script.

When using either the PowerShell or template-based installations, you must determine if the ICA file returned by StoreFront contains an IP address or Fully Qualified Domain Names (FQDNs). If you are unsure, open PowerShell on your Delivery Controller and run the **GetBroker-Site** command. You might have to first run the Add-PSSnapin (**asnpCitrix.***) command and check the **DnsResolutionEnabled** setting, as shown in the below graphic.



Related Links

- ESP
- Configure using the Progress Kemp PowerShell Script
- Configure using the Progress Kemp Template

ESP

ESP

The Progress Kemp Edge Security Pack (ESP) is the LoadMaster's Frontend Authentication engine. The currently supported authentication methods for Citrix StoreFront are Form Based (if LDAP or RADIUS is configured) or SAML for Single Sign On. Various RADIUS MFA (Multi-Factor Authentication) and SAML MFA solutions are supported.

- ◦ For SAML authentication, you must configure using the PowerShell script and configure SAML on your StoreFront server. To configure StoreFront servers for SAML, refer to this knowledge base article from Citrix: How to configure SAML Authentication - Manual Configuration?
- SAML for StoreFront also requires a "Federated Authentication Service" (FAS). This is to prevent your application requesting credentials after connecting. To configure, refer to this Citrix knowledge base article: Federated Authentication Service.
- Your IDP must be configured for two applications. One for the LoadMaster and one for StoreFront. This is

because they both require two different response URLs. The LoadMaster URL is **/Citrix/STOREWeb**, and the StoreFront URL is **/Citrix/StoreAuth/SamlForms/ServiceProvider/Metadata**.

- ◦ For more information on SAML for LoadMaster, refer to the SAML Feature Description.

Configure using the Progress Kemp PowerShell Script

Configure using the Progress Kemp PowerShell Script

Progress Kemp recommends configuring your Citrix Environment using PowerShell. The Progress Kemp PowerShell script is included in the zip file downloaded from the Citrix Virtual Apps and Desktops (StoreFront) web page. The PowerShell script currently requires the use of IP addresses to identify the StoreFront and VDA/VDI servers. In most scenarios we will need the full DHCP scope allocated for your VDA/VDI servers because a specific Secure Listener will be created for each VDA/VDI IP or FQDN.

Install the Progress Kemp PowerShell Module

For further information on the PowerShell API, refer to the PowerShell Interface Description.

You can download the PowerShell wrapper from this page: LoadMaster PowerShell API Wrapper.

You can verify the **Kemp.LoadBalancer.Powershell** module has been properly installed using the Microsoft PowerShell command **GET-Module**. You should see a module named **Kemp.LoadBalancer.Powershell** in the list of modules returned when executing this command.

Related Links

- Installing a New Citrix Workload

Installing a New Citrix Workload

Installing a New Citrix Workload

There are two Progress Kemp PowerShell scripts. One script will initially configure a LoadMaster for Citrix Virtual Apps and Desktops. The second script adds additional VDI servers to an existing Citrix environment. Both scripts are intended to be edited before they are run. There is a section titled **Configure Variables** in the script that needs to be updated to match your environment.

When the PowerShell script has completed, scroll through the log file for any HTTP Error Return Codes such as, **401** or **422**. The log file is located in the current working PowerShell directory.

Before running the script to create the Citrix service, edit the script and modify the variables using the comments in the script for instructions.

In addition to modifying the script, ensure the following files are in the working directory:

- Text file called **vdiservers.txt** containing all VDI server IP addresses or VDI FQDNs. It is recommended to include your full DHCP scope for your Citrix Machine Catalogue
- Text file called **storefront.txt** containing the IP addresses of your StoreFront servers
- TLS certificate in ".pfx" or ".p12" format to use for the Citrix service
- If there are additional certificates in the validation chain, you must add these manually to the LoadMaster after running the script.
- SAML configuration requires you to have your IDP Metadata XML file and your IDP token signing certificate

When you have finished the configuration, continue to the Citrix StoreFront Settings section.

Configure using the Progress Kemp Template

Configure using the Progress Kemp Template

Adding Virtual Services can be both repetitive and prone to error. Progress Kemp have developed a general template mechanism that provides consistency and ease-of-use when creating Virtual Services.

Using templates to set up and configure a Virtual Service is a two-stage process. Initially, you must import the template into the LoadMaster. When imported, you can use the templates when adding a new Virtual Service.

This document outlines the procedure to import the Progress Kemp Citrix Virtual Apps or Desktops template and configure it to control the flow of browser traffic and Citrix Workspace/Receiver traffic. The template creates Virtual Services, Secure Listeners, and content rules.

The downloaded template file contains the following templates:

- **Citrix StoreFront Gateway - With HTML5:** Handles Citrix Virtual Apps and Desktops traffic including Citrix StoreFront Gateway, HTTP redirect, and Connection Server VDI Listeners. Listener decrypts and forwards to VDI on ICA port 2598 or HTML 5 on port 8008.
- **Citrix StoreFront Gateway - Without HTML5:** Handles Citrix Virtual Apps and Desktops traffic including Citrix StoreFront Gateway, HTTP redirect, and Connection Server VDI Listeners. Listener decrypts and forwards to VDI on ICA on port 2598.
- **Citrix StoreFront Gateway - VDA-Encryption:** Handles Citrix Virtual Apps and Desktops traffic including Citrix StoreFront Gateway, HTTP redirect, and Connection Server VDI Listeners. Listener decrypts and re-encrypts to VDI on ICA port 443 or HTML 5 on port 443.
- **Citrix StoreFront Internal:** This template handles internal StoreFront connections. No rewriting of the ICA file occurs. The majority of this document covers external configurations. For further details on internal configurations, refer to the Citrix StoreFront Internal Configuration section.

Related Links

- Template
- Global Settings

- Import the Template
- Citrix StoreFront Internal Configuration
- Create and Update the Virtual Services and Secure Listeners (External)
- Secure Listeners
- Modify the Content Rules
- SSL Certificate

Template

Template

Progress Kemp has developed a template containing our recommended settings for this workload. You can install this template to help create Virtual Services (VSs) because it automatically populates the settings. You can use the template to easily create the required VSs with the recommended settings. For some workloads, additional manual steps may be required such as assigning a certificate or applying port following. These steps are covered in the document, if needed.

You can remove templates after use and this will not affect deployed services. If needed, you can make changes to any of the VS settings after using the template.

Download released templates from the following page: LoadMaster Templates.

For more information and steps on how to import and use templates, refer to the Virtual Services and Templates, Feature Description.

Global Settings

Global Settings

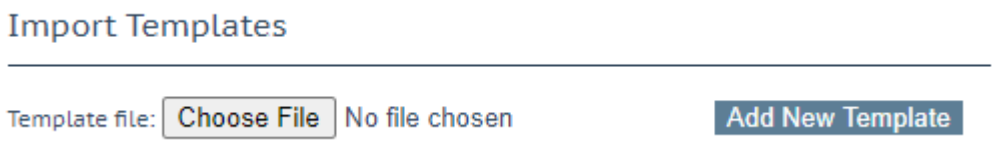
You must enable the global **Share SubVS Persistence** option. This change is necessary to prevent a double authentication prompt. By default, each SubVS of a Virtual Service has an independent persistence table. Enabling **Share SubVS Persistence** allows the SubVS to share this information.

To enable **Share SubVS Persistence**, follow the steps below:

1. In the LoadMaster User Interface (UI), navigate to **System Configuration > Miscellaneous Options > L7 Configuration**.
2. Select the **Share SubVS Persistence** check box.
3. Reboot the LoadMaster after enabling **Share SubVS Persistence** option to activate it (**System Configuration > System Administration > System Reboot > Reboot**).

Import the Template

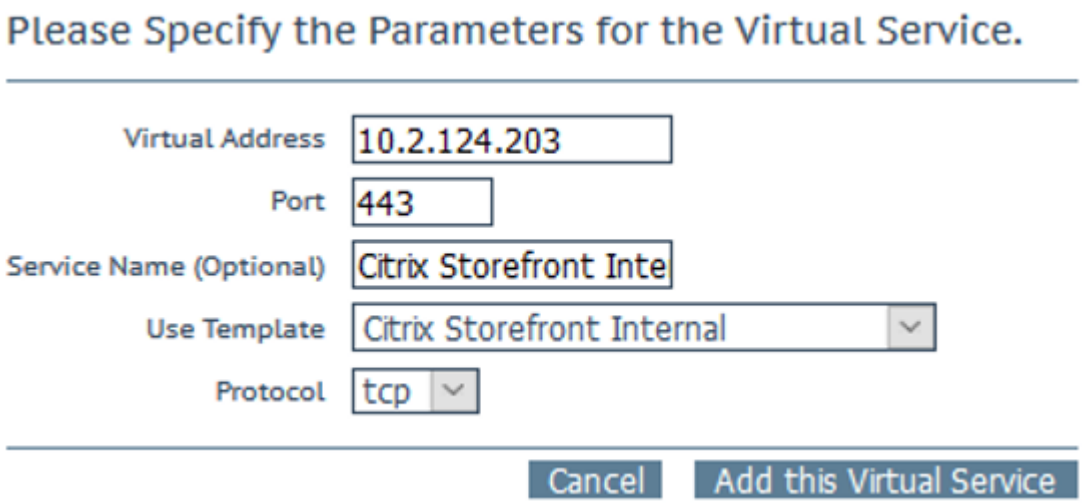
Import the Template



You can import the Citrix StoreFront Gateway template on the LoadMaster through the **Manage Templates** screen located under **Virtual Services** in the main menu of the LoadMaster User Interface (UI).

Citrix StoreFront Internal Configuration

Citrix StoreFront Internal Configuration



To configure Citrix Virtual Apps internally, select the **Citrix StoreFront Internal** template from the **Use Template** drop-down list.

The template is configured for SSL offloading. You can disable this if needed (**Virtual Services > View/ Modify Services > Modify > SSL Properties** > disable **SSL Acceleration**).

Add your StoreFront Severs to the Virtual Service under the **Real Servers** section of the Virtual Service **Modify** screen. No additional configuration is required.

Create and Update the Virtual Services and Secure Listeners (External)

Create and Update the Virtual Services and Secure Listeners (External)

When adding a new Virtual Service, you can select the template from the list of installed templates in the **Use Template** drop-down list. Selecting a template populates the **Port** and **Protocol** of the Virtual Service. When you click **Add this Virtual Service**, the Virtual Service is created, and the attributes of the Virtual Service are automatically configured by the template. Once loaded, you can modify the Virtual Service in the same way as a manually created one.

Related Links

- Authentication
- Citrix StoreFront Gateway Virtual Service

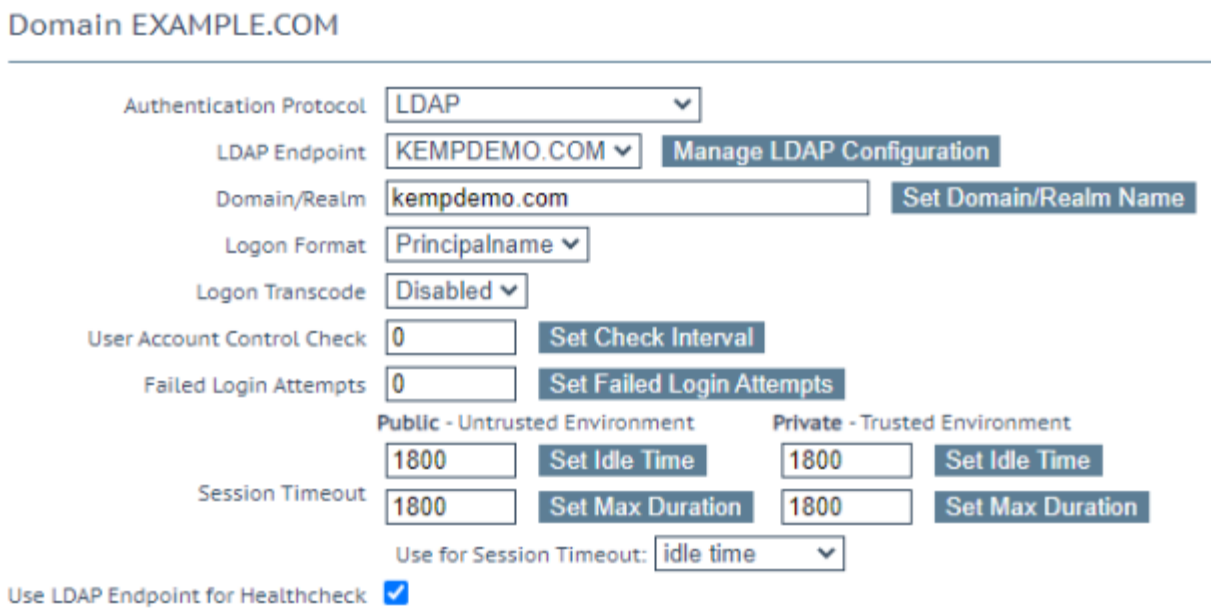
Authentication

Authentication

When a client connects to Citrix StoreFront using a browser, they must authenticate using Progress Kemp ESP front-end authentication. This is handled in the StoreFront Browser Auth ESP Virtual Service.

Begin by navigating to **Certificates & Security > LDAP Configuration** in the LoadMaster UI. Create a new LDAP endpoint by typing a valid name and clicking **Add**. No special characters or spaces are allowed. Ensure to note the name of the LDAP endpoint because this is required in the next step. Specify the parameters for the LDAP endpoint. For further details on how to configure an LDAP endpoint, refer to the following Knowledge Base article: How to configure an LDAP endpoint.

After configuring the LDAP endpoint, go to **Virtual Services > Manage SSO** and add a new client-side configuration with an appropriate name.



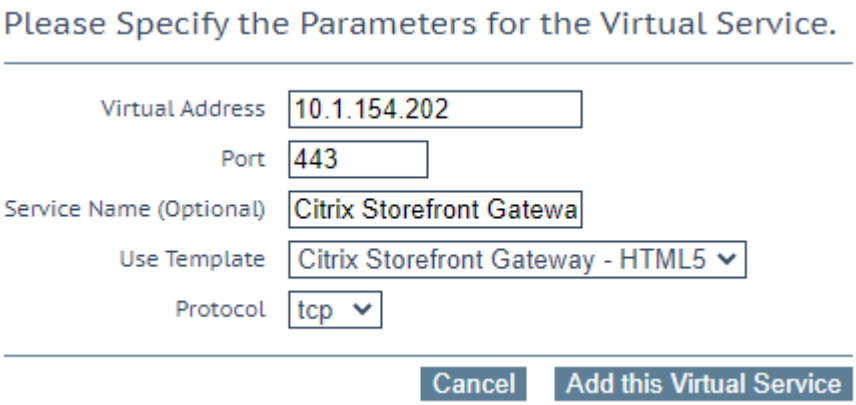
Then, select the **LDAP Endpoint** as configured previously and the **Domain/Realm** as per your Domain Controller settings.

Note: Idle timeout only functions correctly on Virtual Apps & Desktops 7 StoreFront 1912 LTS or later. Idle timeout should be set to a value greater than your Citrix StoreFront where default is 20 minutes. For example, in the screenshot above the idle timeout is set to **1800** seconds (30 minutes). When the idle timeout expires on StoreFront, it sends a logoff string which the LoadMaster will detect and clear the session.

If you are unable to upgrade to StoreFront 1912 set the idle timeout to a full working day on both the LoadMaster and "Sessionstate" on your StoreFront servers (refer to the Appendix for further details on this) otherwise clients must refresh their browser to re-authenticate before launching an application.

Citrix StoreFront Gateway Virtual Service

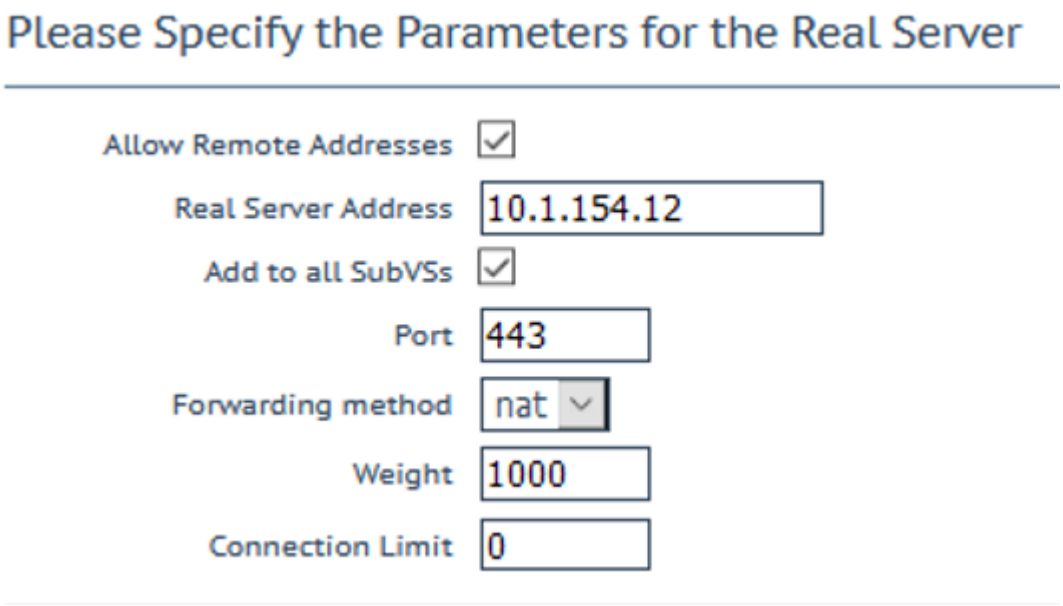
Citrix StoreFront Gateway Virtual Service



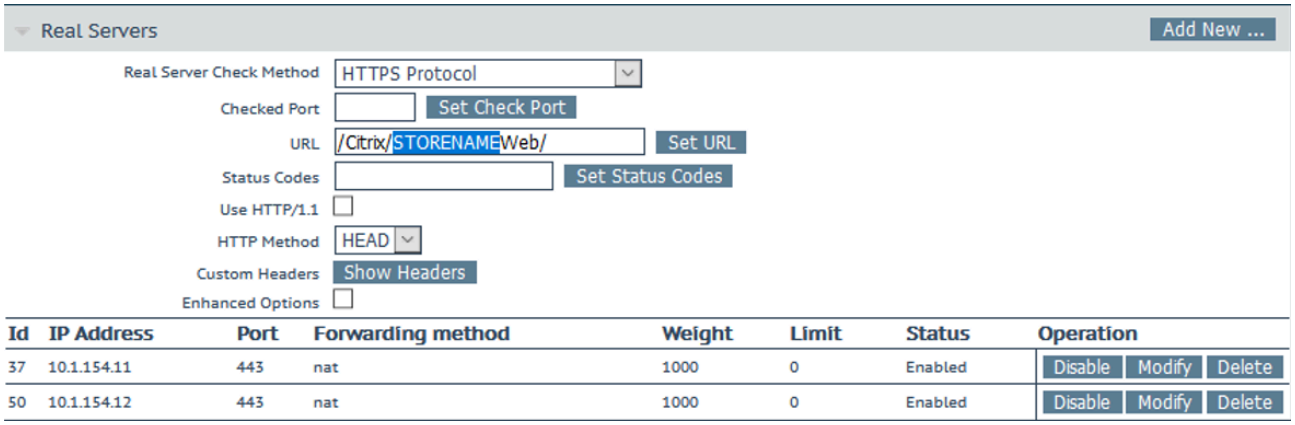
From the **Virtual Services > Add New** in the main menu of the LoadMaster UI, select a template that meets your Citrix Virtual Apps and Desktops environment.

This Virtual Service IP address will be configured for your external DNS record, for example **citrix.domain.com 10.1.154.202** which will resolve to a Public IP address where it will be NATed to the Virtual Service IP address. Enter the **Virtual Address** and click **Add this Virtual Service**.

The **Citrix StoreFront Gateway** Virtual Service consists of either two, three, four, or five SubVSs depending on the selected template. These SubVSs are used to authenticate and rewrite your ICA file. The template also creates multiple Secure Listeners which are used to connect securely to your VDI servers.

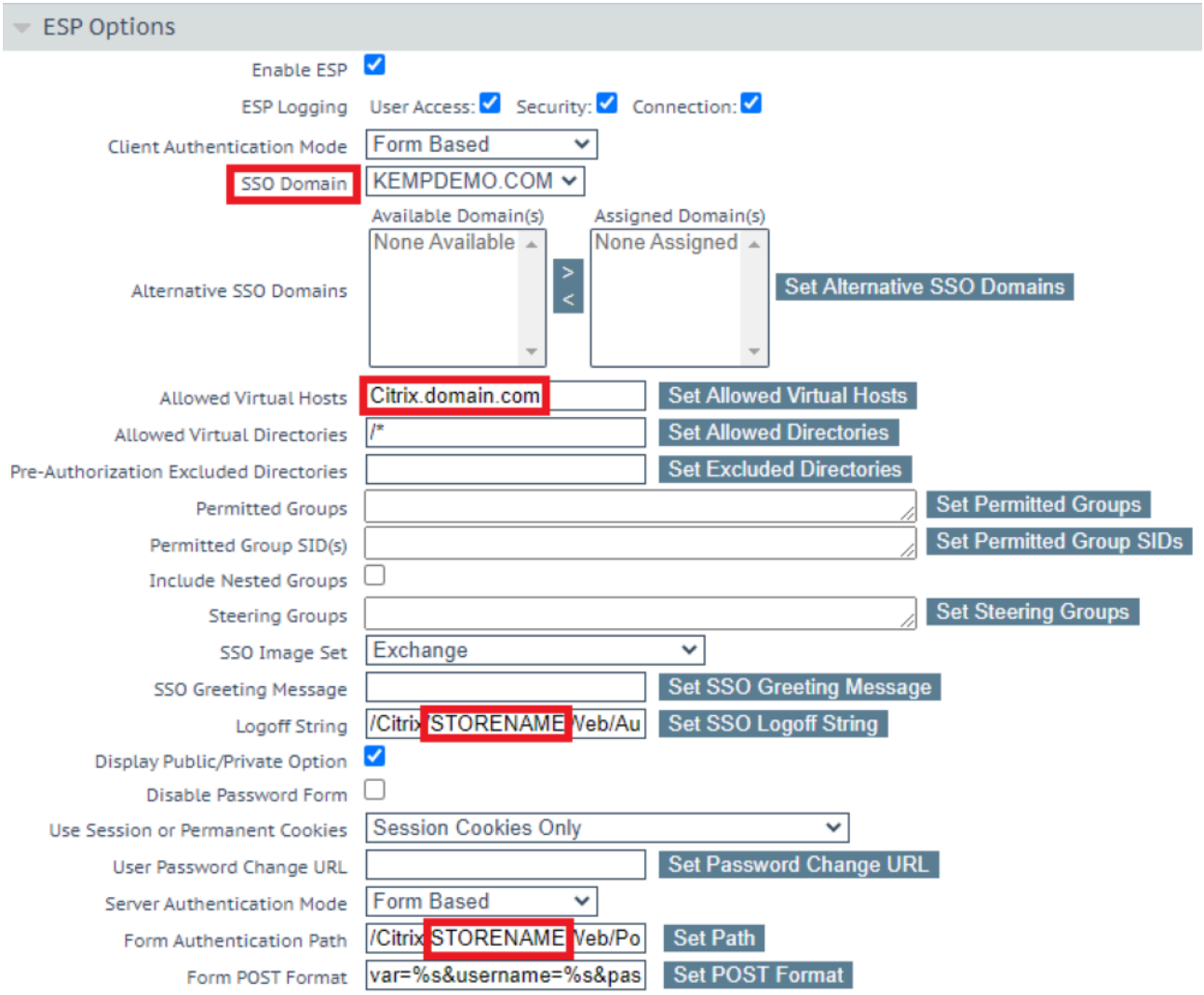


Expand the **SubVSs** section and click **Modify** on the **StoreFront Browser Auth ESP** SubVS. Expand the **Real Servers** section and click **Add New** to add your StoreFront servers. Select the **Add to All SubVSs** check box (as shown above) so your StoreFront servers will be added to all SubVSs.



After Adding your StoreFront servers, update the health check Citrix Store Name **URL**. Replace **STORENAME** with the name of your Store. Modify all SubVSs to update the health check URL (as shown above).

Note: The **STORENAME** is case sensitive.



On the **StoreFront Browser Auth ESP & StoreFront Workspace-Receiver Auth ESP** SubVS, update the **ESP Options** settings of **SSO Domain**, **Allowed Virtual Hosts**, **Logoff String** and **Form Authentication Path**. For the **Logoff String** and **Form Authentication Path**, replace **STORENAME** with your StoreFront name (as shown above).

For non-ESP deployments, simply update your health check **URL** in each SubVS.

Note: The **STORENAME** is case sensitive.

Logoff String: /Citrix/STORENAMEWeb/Authentication/Logoff

Form Authentication Path: /Citrix/STORENAMEWeb/PostCredentialsAuth/Login

Secure Listeners

Secure Listeners

Each of these secure listeners appear as a Virtual Service under **Virtual Services > View/Modify Services** in the LoadMaster UI. Modify each of the Virtual Services to add a Real Server (back-end VDI server) which will point to the corresponding VDI IP address that the template created and will be modified in the Modify the Content Rules section.

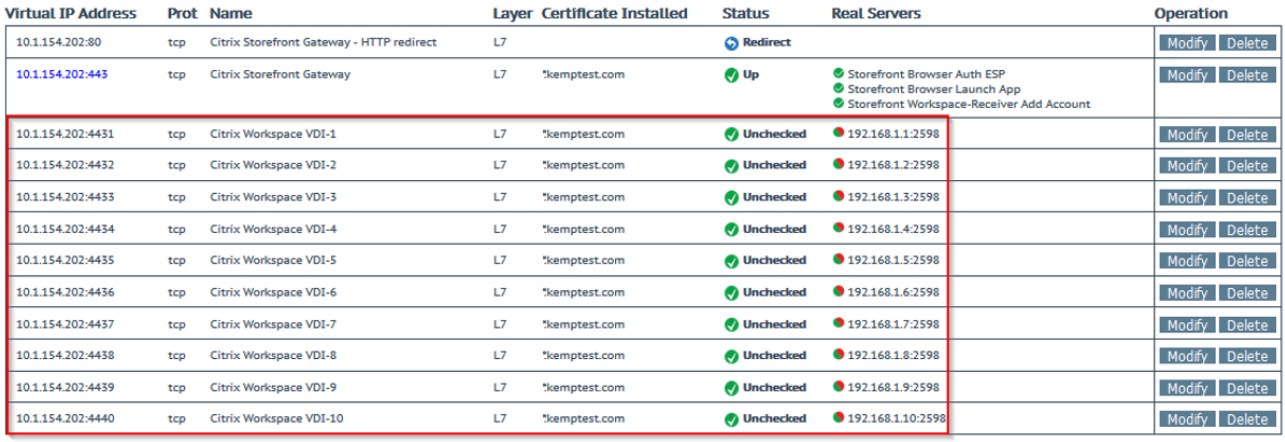
Each Secure Listener Virtual Service offloads/decrypts the encrypted traffic and forwards on port **2598** for Workspace/Receiver and port **8008** if utilizing HTML5 WebSockets.

Below is an example of how 10 VDI Secure Listeners are mapped to specific VDI servers.

Citrix StoreFront Gateway Template

Workspace VDI:

External VIP	VDI Servers
10.1.154.202:4431	-> 192.168.1.1:2598
10.1.154.202:4432	-> 192.168.1.2:2598
10.1.154.202:4433	-> 192.168.1.3:2598
10.1.154.202:4434	-> 192.168.1.4:2598
10.1.154.202:4435	-> 192.168.1.5:2598
10.1.154.202:4436	-> 192.168.1.6:2598
10.1.154.202:4437	-> 192.168.1.7:2598
10.1.154.202:4438	-> 192.168.1.8:2598
10.1.154.202:4439	-> 192.168.1.9:2598
10.1.154.202:4440	-> 192.168.1.10:2598



Virtual IP Address	Prot	Name	Layer	Certificate Installed	Status	Real Servers	Operation
10.1.154.202:80	tcp	Citrix Storefront Gateway - HTTP redirect	L7		Redirect		Modify Delete
10.1.154.202:443	tcp	Citrix Storefront Gateway	L7	*kemptest.com	Up	Storefront Browser Auth ESP Storefront Browser Launch App Storefront Workspace-Receiver Add Account	Modify Delete
10.1.154.202:4431	tcp	Citrix Workspace VDI-1	L7	*kemptest.com	Unchecked	192.168.1.1:2598	Modify Delete
10.1.154.202:4432	tcp	Citrix Workspace VDI-2	L7	*kemptest.com	Unchecked	192.168.1.2:2598	Modify Delete
10.1.154.202:4433	tcp	Citrix Workspace VDI-3	L7	*kemptest.com	Unchecked	192.168.1.3:2598	Modify Delete
10.1.154.202:4434	tcp	Citrix Workspace VDI-4	L7	*kemptest.com	Unchecked	192.168.1.4:2598	Modify Delete
10.1.154.202:4435	tcp	Citrix Workspace VDI-5	L7	*kemptest.com	Unchecked	192.168.1.5:2598	Modify Delete
10.1.154.202:4436	tcp	Citrix Workspace VDI-6	L7	*kemptest.com	Unchecked	192.168.1.6:2598	Modify Delete
10.1.154.202:4437	tcp	Citrix Workspace VDI-7	L7	*kemptest.com	Unchecked	192.168.1.7:2598	Modify Delete
10.1.154.202:4438	tcp	Citrix Workspace VDI-8	L7	*kemptest.com	Unchecked	192.168.1.8:2598	Modify Delete
10.1.154.202:4439	tcp	Citrix Workspace VDI-9	L7	*kemptest.com	Unchecked	192.168.1.9:2598	Modify Delete
10.1.154.202:4440	tcp	Citrix Workspace VDI-10	L7	*kemptest.com	Unchecked	192.168.1.10:2598	Modify Delete

Once configured, your Virtual Services should resemble the layout shown in the screenshot above.

Citrix StoreFront Gateway - HTML5 Template

Workspace VDI:

External VIP	VDI Servers
10.1.154.202:4431	-> 192.168.1.1:2598
10.1.154.202:4432	-> 192.168.1.2:2598
10.1.154.202:4433	-> 192.168.1.3:2598
10.1.154.202:4434	-> 192.168.1.4:2598
10.1.154.202:4435	-> 192.168.1.5:2598

HTML5 VDI:

External VIP	VDI Servers
10.1.154.202:4436	-> 192.168.1.1:8008
10.1.154.202:4437	-> 192.168.1.2:8008
10.1.154.202:4438	-> 192.168.1.3:8008
10.1.154.202:4439	-> 192.168.1.4:8008
10.1.154.202:4440	-> 192.168.1.5:8008

Virtual IP Address	Prot	Name	Layer	Certificate Installed	Status	Real Servers	Operation
10.1.154.202:80	tcp	Citrix - Storefront Redirect	L7		Redirect		Modify Delete
10.1.154.202:443	tcp	Citrix Storefront Gateway	L7	*kemptest.com	Up	Storefront Browser Auth ESP Storefront Browser Launch HTML5 App Storefront Workspace-Receiver Add Account Storefront Workspace-Receiver Launch App	Modify Delete
10.1.154.202:4431	tcp	Citrix Workspace VDI-1	L7	*kemptest.com	Unchecked	192.168.1.1:2598	Modify Delete
10.1.154.202:4432	tcp	Citrix Workspace VDI-2	L7	*kemptest.com	Unchecked	192.168.1.2:2598	Modify Delete
10.1.154.202:4433	tcp	Citrix Workspace VDI-3	L7	*kemptest.com	Unchecked	192.168.1.3:2598	Modify Delete
10.1.154.202:4434	tcp	Citrix Workspace VDI-4	L7	*kemptest.com	Unchecked	192.168.1.4:2598	Modify Delete
10.1.154.202:4435	tcp	Citrix Workspace VDI-5	L7	*kemptest.com	Unchecked	192.168.1.5:2598	Modify Delete
10.1.154.202:4436	tcp	Citrix HTML5 VDI-1	L7	*kemptest.com	Unchecked	192.168.1.1:8008	Modify Delete
10.1.154.202:4437	tcp	Citrix HTML5 VDI-2	L7	*kemptest.com	Unchecked	192.168.1.2:8008	Modify Delete
10.1.154.202:4438	tcp	Citrix HTML5 VDI-3	L7	*kemptest.com	Unchecked	192.168.1.3:8008	Modify Delete
10.1.154.202:4439	tcp	Citrix HTML5 VDI-4	L7	*kemptest.com	Unchecked	192.168.1.4:8008	Modify Delete
10.1.154.202:4440	tcp	Citrix HTML5 VDI-5	L7	*kemptest.com	Unchecked	192.168.1.5:8008	Modify Delete

Once configured, your Virtual Services should resemble the layout shown in the screenshot above.

Modify the Content Rules

Modify the Content Rules

In the LoadMaster UI, go to **Rules & Checking > Content Rules** from the menu and scroll down to see the Header Modification and Body Modification rules. The template deploys Content Rules starting with **Citrix_** and these are applied to the appropriate Virtual Services.

Related Links

- Header Modifications
- Body Modifications
- Adding Additional VDI Server Listeners
- Deactivate Secure Listeners

Header Modifications

Header Modifications

Header Modification Rules

Name	Rule Type	Options	Header	Pattern	Replacement
AcceptEncoding_30185_12532	Delete Header			Accept-Encoding	
CitrixHTTPS_30185_12532	Add Header		X-Citrix-IsUsingHTTPS		Yes
Citrix_Browser_URL	Modify URL			/^\/$/	/Citrix/STORENAMEWeb/
Citrix_Delete_CtxAithID	Add Header	Only On 3	Set-Cookie		CtxsAuthId=*; expires=Thu, 14-Jun-1990 16:53:03 GMT; path=/Citrix/STORENAMEWeb/; secure
HTTP_200To302_12532	Modify URL			200 OK	301 Moved Permanently
Redirect_Citrix_12532	Add Header		Location		https://Citrix.kemptest.com/Citrix/STORENAMEWeb/

Start by modifying three (3) of the **Header Modification Rules**:

Note: If deploying without ESP, only one rule (**Citrix_Browser_URL**) must be updated.

- **Citrix_Browser_URL:** Replace **STORENAME** with your own store name, including the forward slash.
- **Citrix_Delete_AuthID:** Replace **STORENAME** with your own store name, including the forward slash.
- **Citrix_Redirect:** Replace the full FQDN and path, including the forward slash.

Note: The **STORENAME** is case sensitive.

Body Modifications

Body Modifications

The LoadMaster is going to read the ICA file and take your internal IP address and rewrite it to your external FQDN using a specific secure destination port as outlined in the Secure Listeners section. This is achieved with the following updates to the default body modification rules as shown in the screenshot below.

Body Modification Rules

Name	Options	Pattern	Replacement
Citrix_GatewayAddress_19222	Only On 2 Ignore Case	GatewayAddress	Address
Citrix_HTML5_VDI_01_19222	Ignore Case	Address=192.168.1.1:1494	SSLProxyHost=EXTERNAL.DOMAIN.COM:4436
Citrix_HTML5_VDI_02_19222	Ignore Case	Address=192.168.1.2:1494	SSLProxyHost=EXTERNAL.DOMAIN.COM:4437
Citrix_HTML5_VDI_03_19222	Ignore Case	Address=192.168.1.3:1494	SSLProxyHost=EXTERNAL.DOMAIN.COM:4438
Citrix_HTML5_VDI_04_19222	Ignore Case	Address=192.168.1.4:1494	SSLProxyHost=EXTERNAL.DOMAIN.COM:4439
Citrix_HTML5_VDI_05_19222	Ignore Case	Address=192.168.1.5:1494	SSLProxyHost=EXTERNAL.DOMAIN.COM:4440
Citrix_SSL_On_19222	Ignore Case	SSLEnable=Off	SSLEnable=On
Citrix_Workspace_VDI_01_19222	Ignore Case	Address=192.168.1.1:1494	SSLProxyHost=EXTERNAL.DOMAIN.COM:4431
Citrix_Workspace_VDI_02_19222	Ignore Case	Address=192.168.1.2:1494	SSLProxyHost=EXTERNAL.DOMAIN.COM:4432
Citrix_Workspace_VDI_03_19222	Ignore Case	Address=192.168.1.3:1494	SSLProxyHost=EXTERNAL.DOMAIN.COM:4433
Citrix_Workspace_VDI_04_19222	Ignore Case	Address=192.168.1.4:1494	SSLProxyHost=EXTERNAL.DOMAIN.COM:4434
Citrix_Workspace_VDI_05_19222	Ignore Case	Address=192.168.1.5:1494	SSLProxyHost=EXTERNAL.DOMAIN.COM:4435

In the body response rules, replace the internal IP addresses with your own Citrix VDI server IP addresses, as shown above. Ensure to retain port 1494 - only modify the IP address. In some environments the FQDN is returned. In this case, add the FQDN instead of the IP address while also retaining port 1494. If you are uncertain if the ICA file returns an FQDN or an IP address, complete the following steps:

1. Internally, log in to StoreFront.
2. When it asks to detect Receiver, cancel and select **Already Installed**.
3. Click on an application and download the ICA file.

```
[Calculator]
Address=192.168.1.1:1494
AutologonAllowed=ON
BrowserProtocol=HTTPonTCP
CGPSecurityTicket=On
ClearPassword=D353675A14F3CE
ClientAudio=On
```

4. Open using Notepad and note the **Address=** setting, as shown above.

Body Modification Rules

Name	Options	Pattern	Replacement
Citrix_GatewayAddress_26237	Only On 2 Ignore Case	GatewayAddress	Address
Citrix_SSL_On_26237	Ignore Case	SSLEnable=Off	SSLEnable=On
Citrix_Workspace_VDI_01_26237	Ignore Case	Address=192.168.1.1:1494	SSLProxyHost=EXTERNAL.DOMAIN.COM:4431
Citrix_Workspace_VDI_02_26237	Ignore Case	Address=192.168.1.2:1494	SSLProxyHost=EXTERNAL.DOMAIN.COM:4432
Citrix_Workspace_VDI_03_26237	Ignore Case	Address=192.168.1.3:1494	SSLProxyHost=EXTERNAL.DOMAIN.COM:4433
Citrix_Workspace_VDI_04_26237	Ignore Case	Address=192.168.1.4:1494	SSLProxyHost=EXTERNAL.DOMAIN.COM:4434
Citrix_Workspace_VDI_05_26237	Ignore Case	Address=192.168.1.5:1494	SSLProxyHost=EXTERNAL.DOMAIN.COM:4435
Citrix_Workspace_VDI_06_26237	Ignore Case	Address=192.168.1.6:1494	SSLProxyHost=EXTERNAL.DOMAIN.COM:4436
Citrix_Workspace_VDI_07_26237	Ignore Case	Address=192.168.1.7:1494	SSLProxyHost=EXTERNAL.DOMAIN.COM:4437
Citrix_Workspace_VDI_08_26237	Ignore Case	Address=192.168.1.8:1494	SSLProxyHost=EXTERNAL.DOMAIN.COM:4438
Citrix_Workspace_VDI_09_26237	Ignore Case	Address=192.168.1.9:1494	SSLProxyHost=EXTERNAL.DOMAIN.COM:4439
Citrix_Workspace_VDI_10_26237	Ignore Case	Address=192.168.1.10:1494	SSLProxyHost=EXTERNAL.DOMAIN.COM:4440

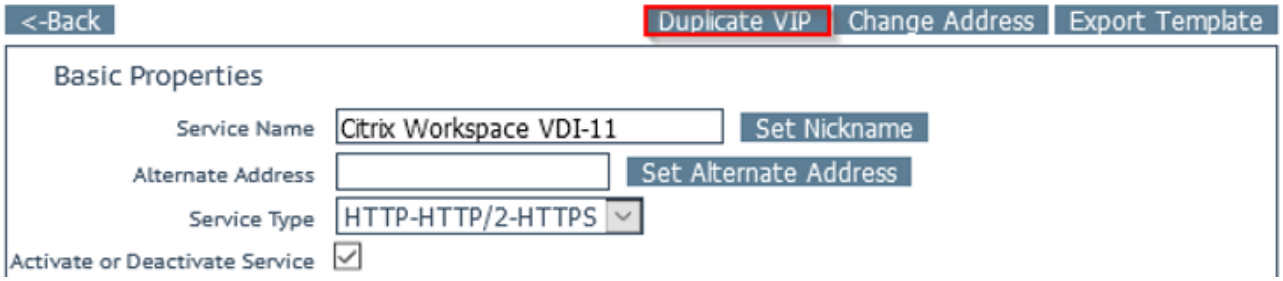
Note: If port **:1494** is not included, then remove it from each of the rules that are shown in the above two screenshots.

In the body modification rules in the LoadMaster UI, change **EXTERNAL.DOMAIN.COM** in the **Replacement text** field to be your external URL, as shown above. Again, ensure you do not change the port number as this is associated with your Secure Listener VDI Virtual Service.

Adding Additional VDI Server Listeners

Adding Additional VDI Server Listeners

You can use the UI to create new VDI listeners and content rules by following these steps:



1. Duplicate an existing Secure Listener. You can do this in the Virtual Service modify screen by clicking **Duplicate VIP**.
2. Set a new name for the duplicated Virtual Service, such as **Citrix - Workspace-ICA VDI-11** and change to a new unique listening port such as **4445**.
3. In the **Real Servers** section, delete the existing Real Server, such as **192.168.1.10**, and add the new VDI server IP address (for example, **192.168.1.11**) or FQDN on port **2598** or port **8008** for HTML5.



4. Duplicate an existing Body Response Rule (go to **Rules & Checking > Content Rules > Duplicate**).



5. Update the **Rule Name**, **Match String**, IP address, and update the port in the **Replacement text** field.
6. Match your new internal IP address and replace it with your secure external URL and with your new unique listening port.
7. Add the rule to the **StoreFront Workspace-Receiver Launch App** SubVS. In the SubVS, go to **Advanced Properties > Show Body Modification Rules** > select the new rule name from the drop-down list and click **Add**.

Deactivate Secure Listeners

Deactivate Secure Listeners

If you do not require all of the Secure Listeners, you can deactivate or delete them. Kemp recommends you simply deactivate as the Listener might be used in the future.

To deactivate a Secure Listener, follow these steps:

1. In the main menu of the LoadMaster UI, go to **Virtual Services > View/Modify Services**.
2. Click **Modify** on the relevant Virtual Service.
3. In the **Basic Properties** section, uncheck the **Activate or Deactivate Service** check box to deactivate the Virtual Service.

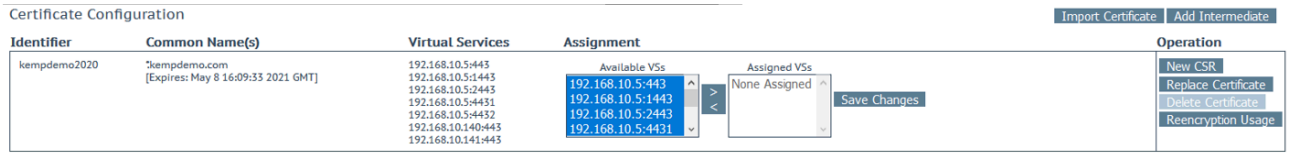
SSL Certificate

SSL Certificate

To enable full end-to-end security and provide the ability to re-encrypt on the Citrix Workspace Browser and

Citrix Workspace Client Virtual Services, you must install a CA signed certificate.

To do this, in the LoadMaster UI go to **Certificates & Security > SSL Certificates**. Click **Import Certificate** and add the appropriate CA signed certificate.



When the certificate is installed, assign it to the StoreFront Gateway Virtual Service and all Secure Listeners.

7

Citrix StoreFront Settings

Citrix StoreFront Settings

Depending on the required features, this section outlines the Citrix StoreFront settings that you must update to support the Progress Kemp solution. These steps are only applicable for external deployments.

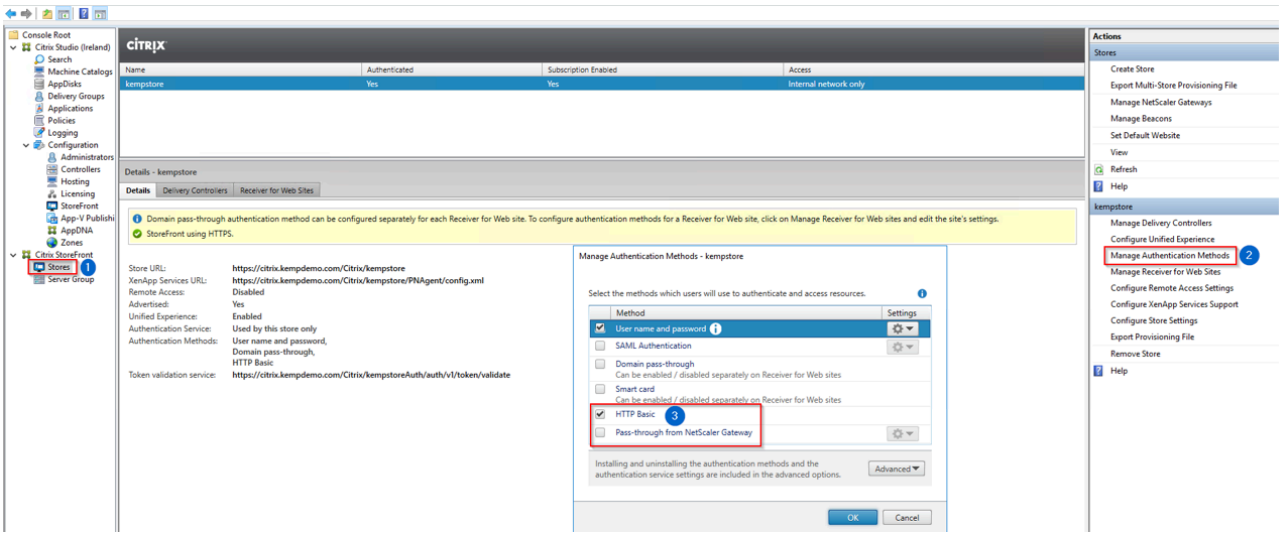
Note: It is not necessary to configure a Remote Access Gateway.

Related Links

- Configure HTTP Basic Authentication
- Configure WebSocket Policy

Configure HTTP Basic Authentication

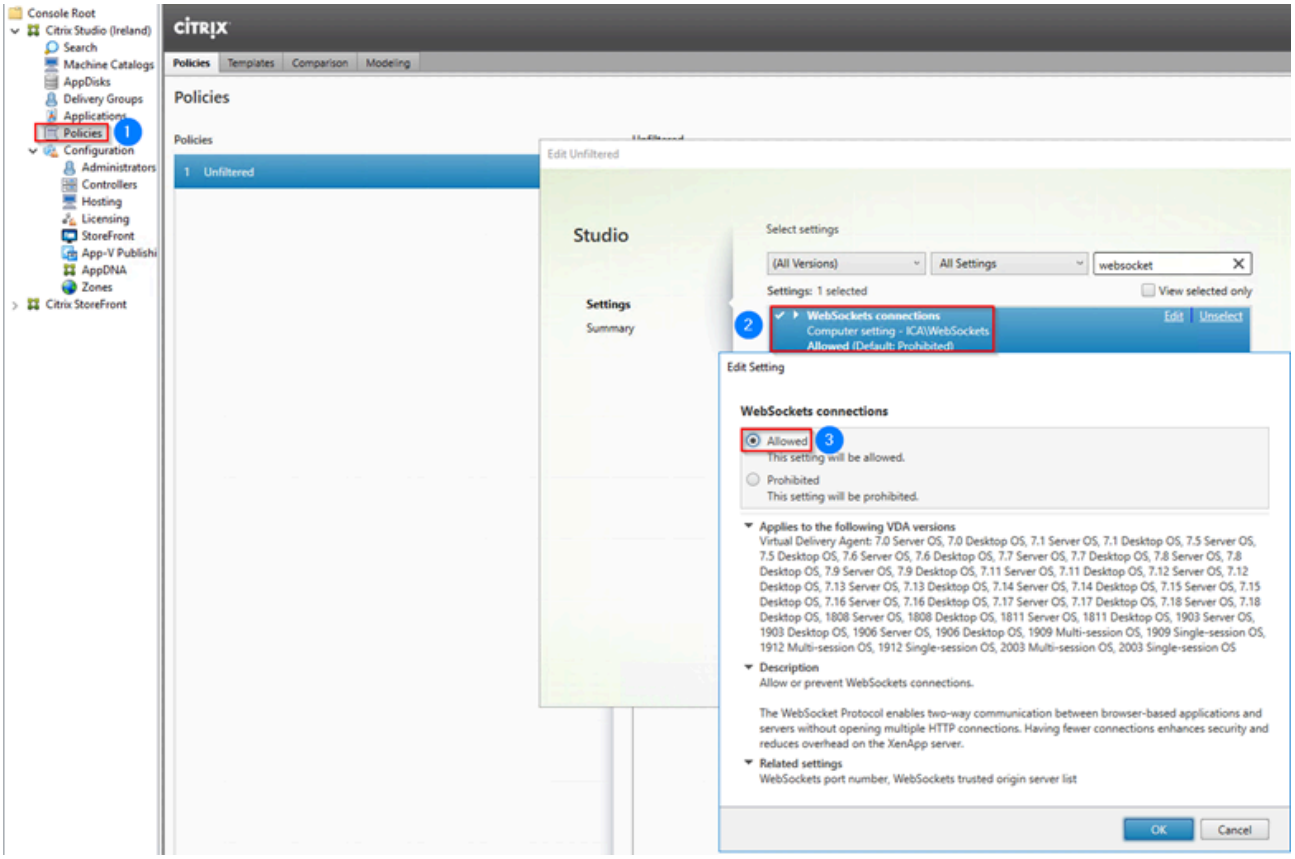
Configure HTTP Basic Authentication



For Form Based authentication, enable **HTTP Basic** authentication. Ensure to propagate the settings.

Configure WebSocket Policy

Configure WebSocket Policy



For HTML5 Web Sockets, enable the WebSockets policy under **Policies**. Ensure to propagate the settings.

8

Testing

Testing

Refer to the following sections for details on testing the Workspace Receiver application, HTML5 Web Socket Connection, and troubleshooting.

Related Links

- Testing Workspace Receiver Application
- Testing HTML5 Web Socket Connection
- Troubleshooting

Testing Workspace Receiver Application

Testing Workspace Receiver Application

Create a DNS record or Host File entry to point to your **Citrix StoreFront Gateway** Virtual Service IP address. You should be greeted with a Progress Kemp logon page. If you are using SAML, you are redirected to your IDP.

After you have successfully authenticated, click **Detect Receiver**. If your Citrix Workspace or Receiver application is installed, your browser should automatically detect it.

From your application store, launch a Virtual application or Virtual Desktop. Your browser should now ask if

you would like to launch your application using Workspace or Receiver. If it is unable to detect either, it will download your ICA file. Locate your ICA File and either double-click or right-click and launch with Workspace or Receiver.

If you receiver an error, refer to the Troubleshooting section.

Note: Please ensure that you are not testing using a Self-Signed Certificate as Workspace/Receiver will close the SSL connection.

Testing HTML5 Web Socket Connection

Testing HTML5 Web Socket Connection

If you have enabled the **WebSocket** policy on your StoreFront server and have configured your Citrix StoreFront Gateway Virtual Service using the HTML5 Template or PowerShell script, you can test by selecting **Use Light Version** upon your initial login, or navigate to **Account Settings > Change Citrix Receiver > Use Light Version**.

From your application store, launch a Virtual application or Virtual Desktop. Your browser should now launch your application from a new browser tab.

If you receive an error, refer to the Troubleshooting section.

Troubleshooting

Troubleshooting

For help with troubleshooting, refer to the following Knowledge Base article: How To - Troubleshoot StoreFront for Citrix Virtual Apps and Desktops.

9

Appendix

Appendix

This appendix outlines how to set the **Sessionstate** on your StoreFront servers:

1. Go to **C:\inetpub\wwwroot\Citrix\STORENAME\web.conf**.

```
</container>
<appSettings />
<!--    For a description of web.config changes for .NET 4.5 see http://go.microsoft.com/fwlink/?LinkId=235367.    The following attributes can be set on
<system.web>
  <!-- minFreeThreads = 88 * N and minLocalRequestFreeThreads = 76 * N where N is the number of logical CPUs -->
  <httpRuntime targetFramework="4.5" executionTimeout="300" appRequestQueueLimit="100" maxRequestLength="4096" enableVersionHeader="false" requestValidat
  <!-- FIPS 140-1 -->
  <machineKey validationKey="AutoGenerate,IsolateApps" decryptionKey="AutoGenerate,IsolateApps" validation="HMACSHA256" decryption="AES" />
  <!--             Set compilation debug="true" to insert debugging            symbols into the compiled page. Because this            affects performa
  <compilation targetFramework="4.5">
    <assemblies>
      <add assembly="System.Web.Mvc, Culture=neutral, PublicKeyToken=31BF3856AD364E35" />
      <add assembly="System.Web.Abstractions, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31BF3856AD364E35" />
      <add assembly="System.Web.Routing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31BF3856AD364E35" />
    </assemblies>
  </compilation>
  <customErrors mode="RemoteOnly" />
  <!-- Tracing disabled by default to improve performance. -->
  <trace enabled="false" localOnly="true" pageOutput="false" requestLimit="1000" mostRecent="true" writeToDiagnosticsTrace="true" traceMode="SortByTime"
  <pages controlRenderingCompatibilityVersion="3.5" clientIDMode="AutoID">
    <namespaces>
      <add namespace="System.Web.Mvc" />
      <add namespace="System.Web.Mvc.Ajax" />
      <add namespace="System.Web.Mvc.Html" />
      <add namespace="System.Web.Routing" />
      <add namespace="System.Linq" />
      <add namespace="System.Collections.Generic" />
    </namespaces>
  </pages>
  <sessionState timeout="600" />
  <caching>
    <outputCacheSettings>
      <outputCacheProfiles>
```

2. Locate **sessionState timeout** and set it to **600** minutes (10 hours).