



Citrix Service Provider Cloud Reference Architecture

Leveraging Citrix Service Provider technologies to deliver Secure Digital
Workspaces

Version 1.0

Contents

Contents	2
1. Executive Summary	4
2. What's new?	5
3. Introduction and Scope	6
4. Overview	7
4.1 Citrix Cloud	7
4.2 Citrix Workspace	7
4.3 Citrix Virtual Apps and Desktops	7
4.4 Cloud Connector	7
5. Architecture Models for Citrix Service Providers	8
5.1 Citrix Virtual Apps and Desktops Service for CSP	8
5.2 Security and Isolation	9
External Access Security	9
Storage Security	9
Tenant Isolation	9
5.3 Multi-tenant Architecture Models	10
5.3.1 Shared Resource Location	10
5.3.2 Dedicated Resource Location	11
5.4 Private Workspace (Non-Multi-tenant)	13
5.5 Combination of Different Architecture Models	13
5.6 Workspace Experience and Authentication	14
5.6.1 Active Directory	14
5.6.2 Time-Based One-Time Password	14
5.6.3 Azure Active Directory	14
5.6.4 Citrix Gateway	14
5.6.5 OKTA	14
5.6.5 Cloud Federated Authentication Service	15
6. Deployment Considerations	16
6.1 Datacenters	17
6.2 Microsoft Azure	17
6.3 Amazon Web Services	17
6.4 Google Cloud	18
7. Deployment Steps	19
7.1 Onboard a Customer	19

7.1.1 Add a new Customer	19
7.1.2 Invite a Customer	20
7.2 Enable Virtual Apps and Desktops Service to a New Customer.....	21
7.3 Configure Multi-tenant Virtual Apps and Desktops Service for the New Customer	22
7.3.1 Deploy a New Resource Location.....	22
7.3.2 Define Hosting Connection	23
7.3.3 Configure Machine Catalogues for the New Customer	25
7.3.4 Create Delivery Groups for the New Customer	26
7.4 Configure Federated Domain for the New Customer	28
7.5 Subscribe Customer User Groups to Offerings	29
7.6 Configure Tenant Workspace.....	30
7.6.1 Access URL.....	31
7.6.2 Authentication.....	31
7.6.3 Appearance	32
7.7 User Login to Workspace	32
8. Performance and Monitoring.....	33
8.1 Director.....	33
8.2 Citrix Analytics Service	34
9. Appendix.....	35
Common Abbreviations.....	35
10. References.....	35

1. Executive Summary

The Citrix® Service Provider (CSP) Reference Architecture on Citrix Cloud uses the next generation of cloud service delivery approach, provides guidance on deployment architectures that scale easily while increasing user centric mobility for an expanding customer base.

Citrix Cloud enables the delivery of Microsoft® Windows® and Linux® workspaces with people-centric secure applications and desktops hosted in the Service Provider managed environments from on-premise datacentres to private or public clouds.

Citrix Service Providers can take advantage of the flexible licensing programs to deliver cost-effective services based on subscriber usage.

The reference architecture is easily adapted to meet specific provider and subscriber requirements, allowing Service Providers to deliver a comprehensive set of workspace offerings and price points while simplifying management and scalability.

The cloud-ready services model enables lower infrastructure and administrative costs, speed to market and scalability, greater customer satisfaction, and increased business success.

2. What's new?

This is the first version of the Citrix Service Provider Reference Architecture based on Citrix Virtual Apps and Desktops Service with multi-tenancy support for CSP. This introduces new concepts of hosting customers in shared and dedicated tenant resource locations of partner Cloud service instance, as well as the existing linked partner-customer cloud accounts. The multi-tenant service simplifies the management and license allocation, and allows the integration and deployment of more services and greater integration.

3. Introduction and Scope

This document provides architectural guidance for Citrix Service Providers who utilize Citrix Cloud technologies to offer services to customers and subscribers. The Reference Architecture is intended to assist Service Providers scale from a small subscriber base to an extensive user base shared across multiple tenants and multiple geographies.

The Citrix CSP Reference Architecture is designed to be flexible and can be used to implement hosting environments within virtually any infrastructure, during any phase of implementation.

This documentation describes the design and implementation of the Citrix Cloud solution infrastructure to be vendor agnostic and will use common wording for the specific technology in use.

Multi-tenant resource locations managed by Citrix Service Providers should be highly scalable and available, with great performance and end user experience including the management and incorporation of additional services.

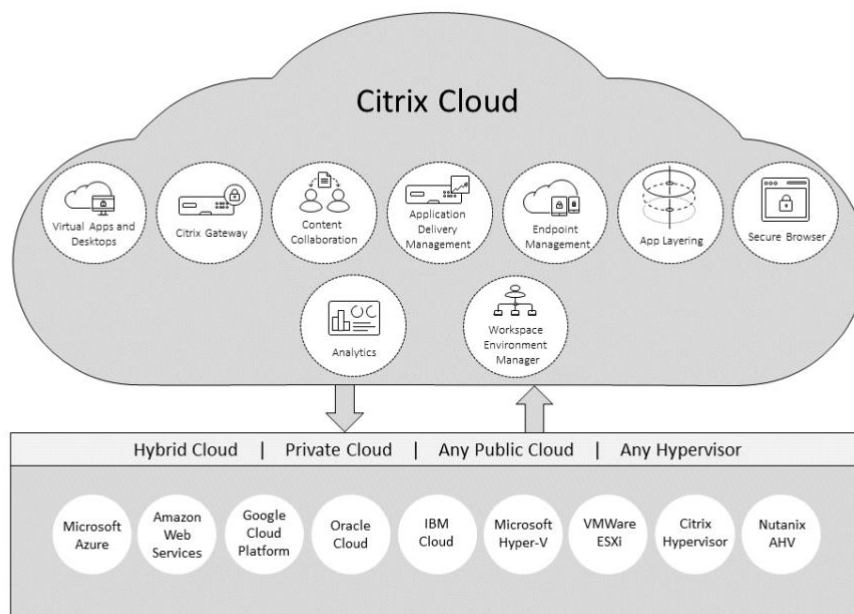
This version of the Reference Architecture focuses on Citrix Virtual Apps and Desktops service for Citrix Service Providers. At time of publication not all Workspace Services support multi-tenancy. We will expand the scope of the reference architecture to cover the overall workspace services for CSPs in future versions.

4. Overview

4.1 Citrix Cloud

Citrix Cloud is a platform that hosts and administers Citrix services, such as Citrix Workspace and Citrix Virtual Apps and Desktops. It connects to hosted resources through the Citrix Cloud Connector on any cloud or infrastructure.

Citrix Cloud allows Citrix Service Providers to create multiple types of workspace hosting environments as resource locations (for example on-premises, public cloud, private cloud, or hybrid cloud).



4.2 Citrix Workspace

Is a unified secure cloud platform managed by Citrix where hosting providers can securely deliver applications and data while maintaining end user experience and productivity in an increasingly mobile workstyle.

4.3 Citrix Virtual Apps and Desktops

Nearly 80% of our Service Providers offer apps and desktops solution to their customers, traditionally these offerings are hosted and managed on-premises. Citrix Virtual Apps and Desktops service makes the Access and Control Layers cloud hosted and managed by Citrix, and provides the flexibility for Service Providers to focus on hosting and managing workloads from their chosen cloud.

4.4 Cloud Connector

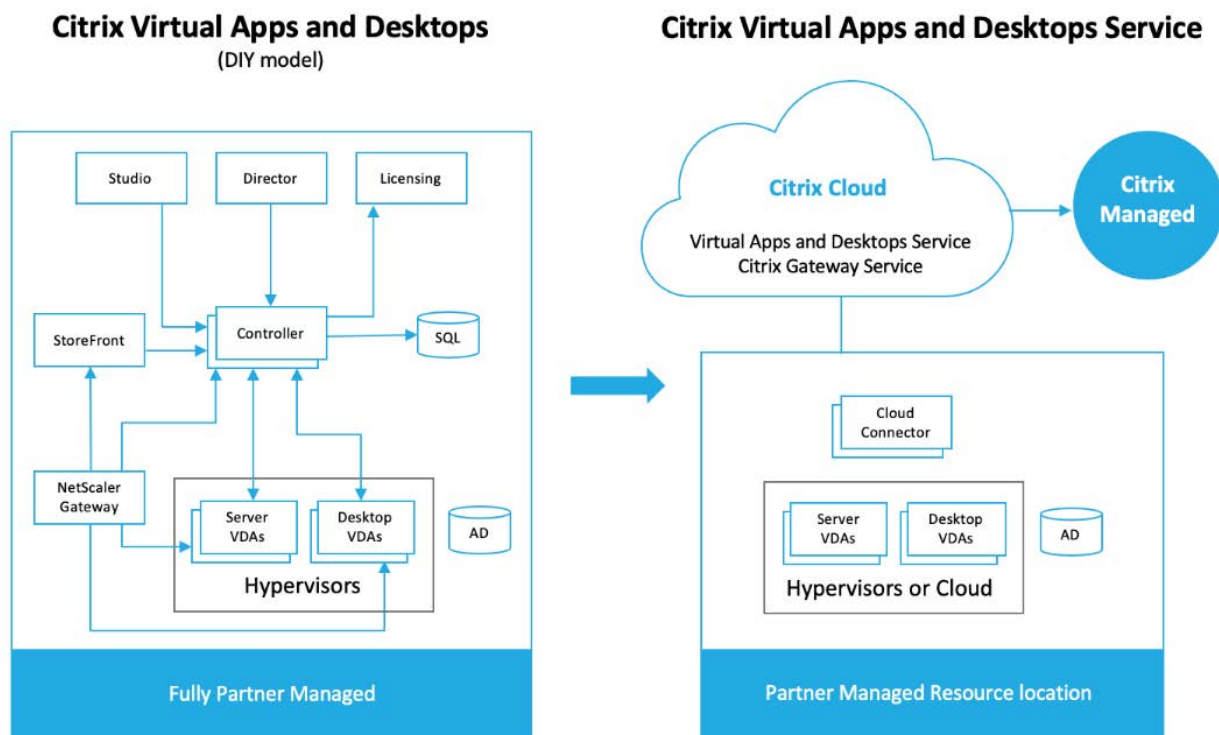
The Cloud Connector is a Citrix component that authenticates and encrypts all communications between Citrix Cloud and Service Provider managed resource location. All communication between Citrix Cloud and the Resource Location environment is encrypted, negating the need for ingress firewall rules.

5. Architecture Models for Citrix Service Providers

Citrix Cloud for Citrix Service Providers (CSPs) is the platform for the delivery and management of Citrix technologies, helping Service providers extend existing hosting deployments or move their customers to a hosted cloud solution. CSPs can create and deploy secure digital workspaces rapidly using Citrix Cloud, while maintaining the control of sensitive data and resources hosted on-prem or in a chosen cloud.

5.1 Citrix Virtual Apps and Desktops Service for CSP

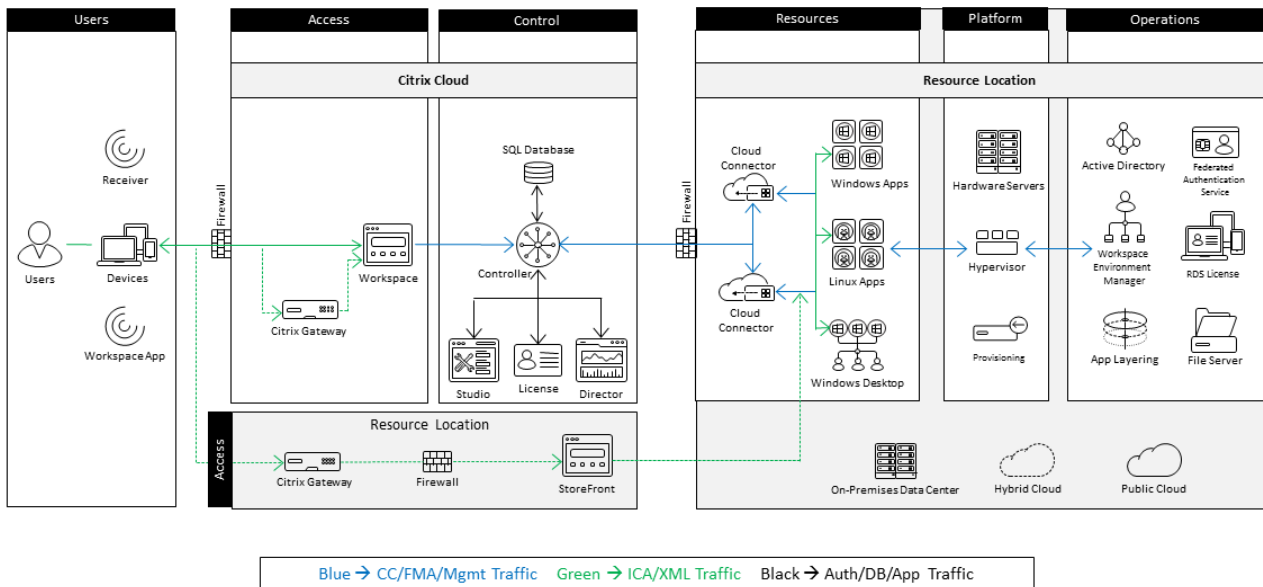
The traditional deployment in a hosting environment for Citrix Virtual Apps and Desktops includes highly available delivery controllers, storefront servers, SQL databases, gateway, and management consoles deployed in the service provider's datacentre along with the Virtual Delivery Agents (VDA). In the Citrix Cloud model for CSP, the management or control plane, and optional access layer (cloud gateway), are managed by Citrix, leaving the Citrix Service Provider to focus on the customers' application data and critical services.



5.2 Security and Isolation

The Citrix Virtual Apps and Desktops Service Architecture consists of layers that connect together to create a complete end-to-end solution for service providers. For general conceptual architecture, and to understand how all layers flow together, please refer to [Citrix Tech Zone](#).

Conceptual Architecture - Citrix Cloud Virtual Apps and Desktops Service



External Access Security

A multi-tenant environment will be isolated from the internet using a blended approach with several complimentary technologies such as Firewalls, Application Delivery Controllers, Packet Filtering, intrusion detection and prevention systems etc. Access to a multi-tenant network from Citrix Cloud is facilitated either by using the Citrix Cloud Connectors or a Citrix Application Delivery Controller and Citrix StoreFront combination.

Management Separation

The core network services for a Service Provider are located in a separate partitioned that allows the hosting of shared services, depending on the services offered, the components of this partition may be: Active Directory Domain Controllers, Backup, Automation Services, DNS etc.

Storage Security

Access to the file repositories of each tenant needs to be separated from other tenants, this can be achieved with using dedicated or shared servers that are protected using security partitions or permissions

Tenant Isolation

Partitioning of the tenants is defined by the level of separation demanded by the customers. Citrix recommends that each tenant is placed into a segregated network using a SDN for their dedicated workloads and complimentary services, ensuring that there are effective security isolation boundaries, with managed networks and IP management and routing

5.3 Multi-tenant Architecture Models

Citrix Cloud Multi-tenant Virtual Apps and Desktops service enables Service Providers to manage multiple customers using the single instance of the service with same Citrix Studio and Director consoles and Role Based Access Control under the partner cloud account. Citrix license management is also centralised for easy allocation.

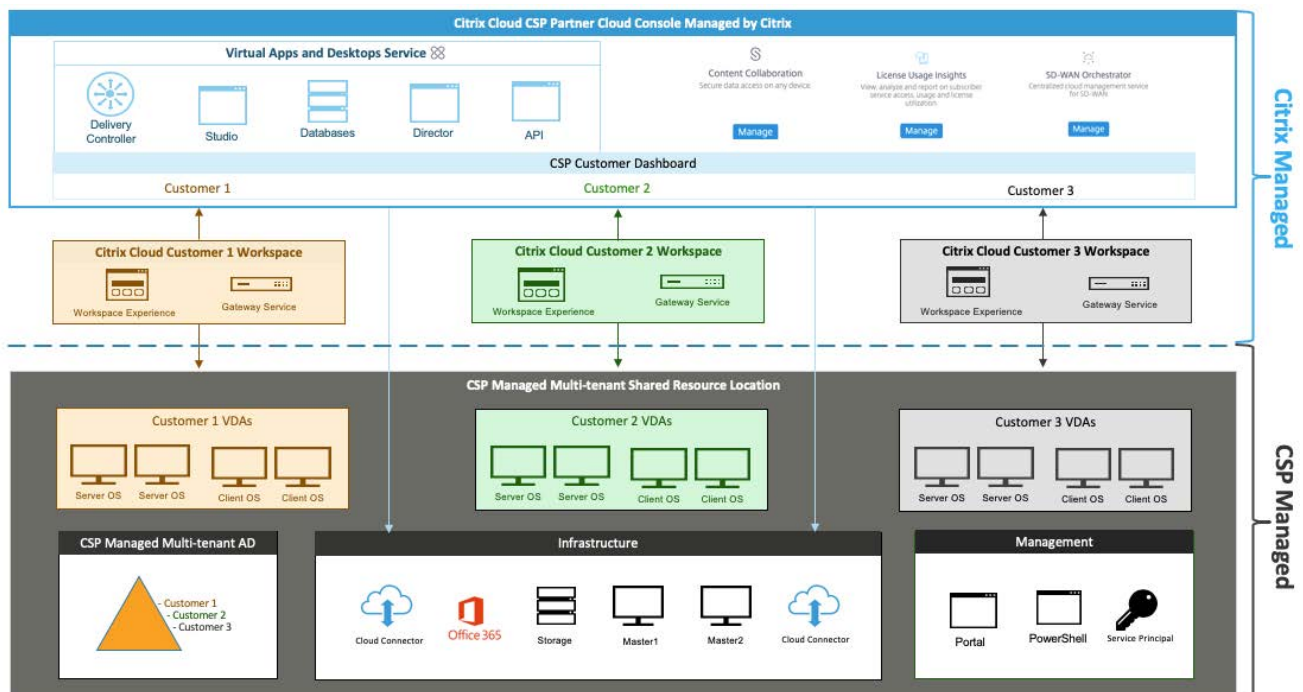
Multi-tenancy capabilities provide economies of scale on a single shared infrastructure while providing the required isolation and data protection. Service Providers can make trade-offs regarding price and features to meet individual tenant requirements.

The tenant isolation in multi-tenant deployments needs to include appropriate nomenclature to clearly define the objects that are shared or dedicated within the management consoles and control plane available to the Service Provider admins, for example *{Tenant}-{Location}-{Group}*.

The Multi-tenant Virtual Apps and Desktops service supports two architecture models:

1. Shared Resource Location for multiple tenants
2. Dedicated resource location per tenant

5.3.1 Shared Resource Location



[Shared Resource Location, showing an overview of the components that can be shared between tenants under Citrix Service Provider's cloud account]

In this multi-tenant architecture model, the customers or tenants of the Service provider share the partner's Citrix Virtual Apps and Desktops service as well as the same resource location, and a hosted Active Directory. Each customer has a dedicated Workspace experience which allows them to customize own workspace configurations including authentication, branding, and Workspace URL to closely align with the customer's business name and brand.

The advantage of this model is to provide the best economics for hosting a wide range of shared customers using shared infrastructure and management components. Service providers are able to elastically scale very easily and incorporate small customers rapidly, the shared resource location can be located on-premises or hosted in a public or private cloud. This option would not allow for hosting at a customer datacentre.

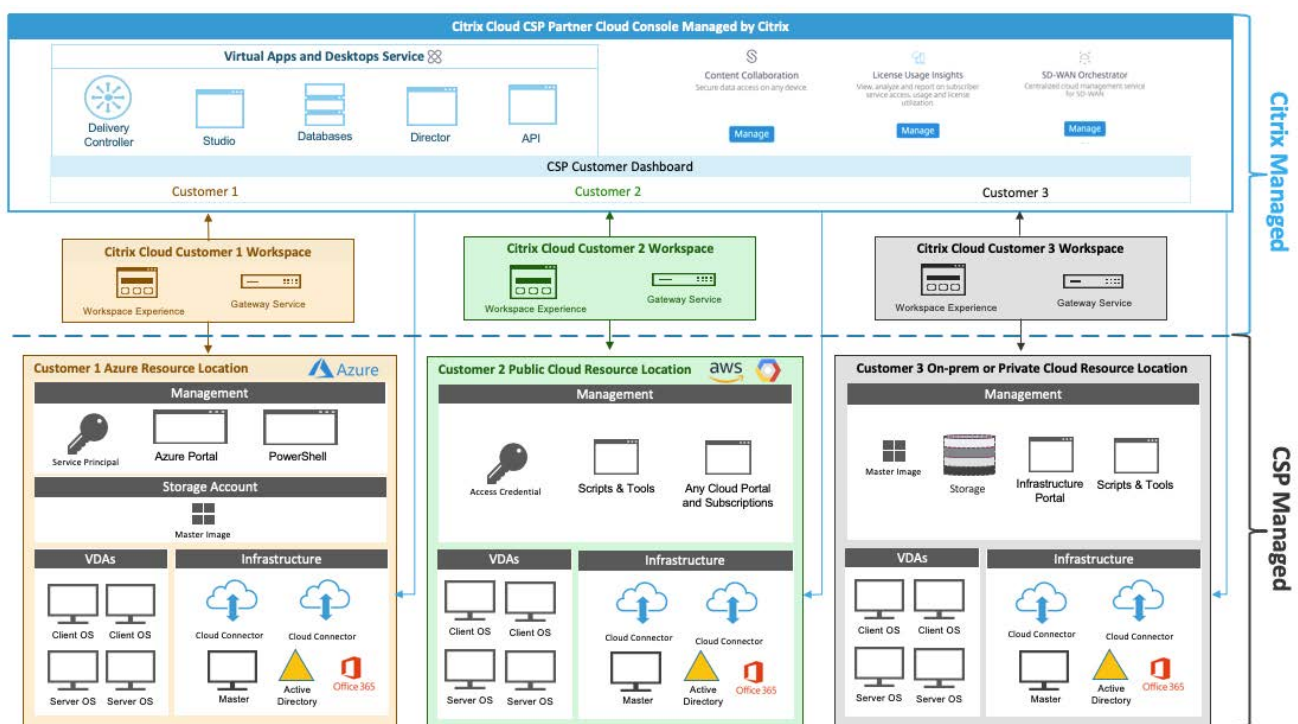
It is recommended that the Machine Catalogs managed in a shared resource location are dedicated per tenant and assigned to specific Customer scope. However, machine catalogs of some common applications for very small tenants may be shared, based on the service provider's discretion. The naming convention also extends to objects managed by the service provider that are contained within the infrastructure. When managing shared Resource Location Delivery Groups, it is highly recommended that they are dedicated per tenant and are assigned with correspondingly named Active Directory Security groups via managing subscribers page on the cloud control plane. Adding individual users to a delivery groups is not recommended due to the high administrative overhead and low scalability.

In summary, under the shared resource location model, each customer has dedicated workspace experience and delivery groups, but share:

- Active Directory
- Resource location and cloud connectors
- Citrix Virtual Apps and Desktops service

The advantages of this model are the best economics, easy and fast cloud transition for existing on-prem multi-tenant AD environment, and good elasticity and scalability. However, it has limitations for integrating custom environments with complex applications and high compliance requirements.

5.3.2 Dedicated Resource Location



[Dedicated Resource Location, showing the dedicated and shared components between tenants under Citrix Service Providers cloud account]

Comparing with the shared resource location model, customers that need more isolation from their hosting provider can use the dedicated Resource location model that shares the Service Provider's Virtual Apps and Desktops service instance, but maintain its isolated active directory, cloud connectors and infrastructure resources.

The dedicated Active Directory and infrastructure resources ensure higher customer isolation and security while shared cloud service instance still maintains the ease of the license allocation and centralised management via the partner control plane, Studio and Monitor console. This model can be hosted using the Service Providers datacenter, public or private cloud locations, or leveraging a customer's datacenter.

Citrix recommends that nomenclature in the Citrix Studio console be rational to indicate information about the workload of the machine catalogs. Each catalog and delivery group should be assigned to specific tenant scope, and similarly named Active Directory Security groups are used instead of adding individual users as subscribers to be assigned to corresponding libraries on partner cloud portal.

This naming convention should be extended to all objects assigned or managed for the tenant including but not limited to hosting connections, Active Directory objects, network subnet, etc.

The dedicated resource location will typically be focused on small to medium customer adoption.

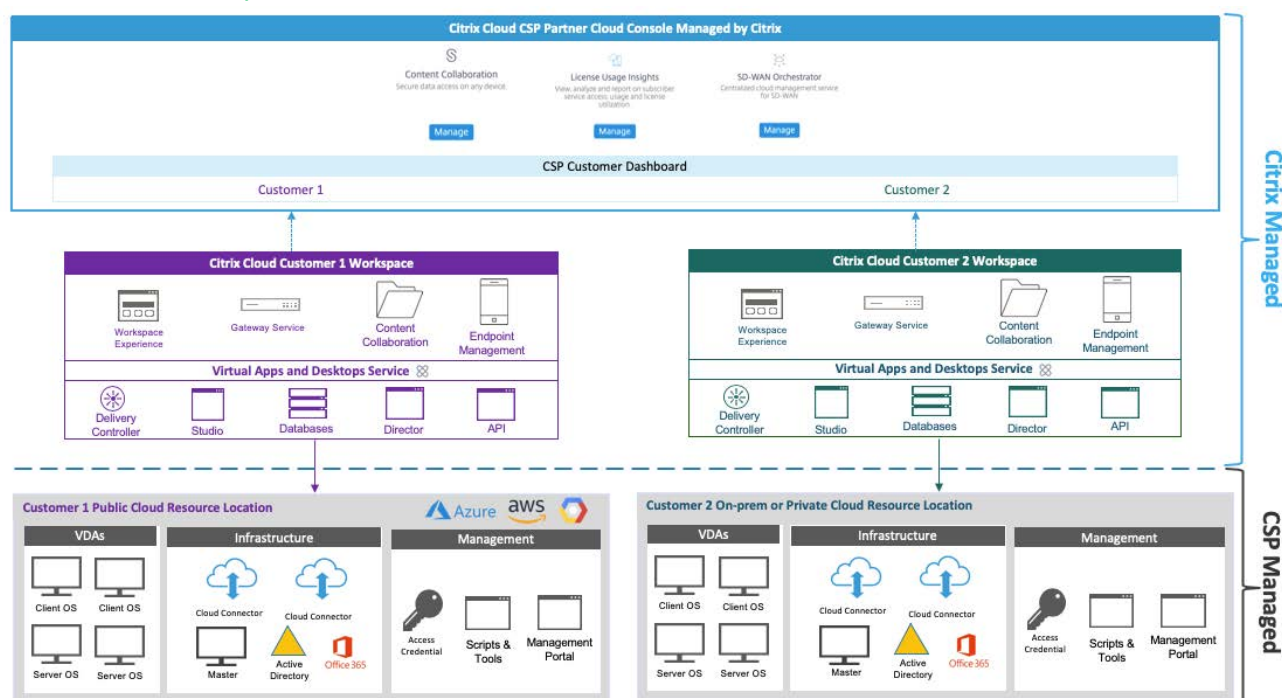
In summary, Customers share CSP's Citrix Virtual Apps and Desktops service under the dedicated resource location model, but each customer has dedicated:

- Workspace experience, resource location, active directory
- Machine Catalog, delivery groups
- Most likely have dedicated subnet/vNet
- Possible Hosting Connection and different cloud location

For very small customers, it is not the most economic model, however there are many advantages of this architecture model:

- Less administration cost when compared to complete private isolation
- Centralized management and easy license allocation
- Supports hybrid and multi cloud adoption
- Good flexibility and scalability
- Balanced approach and suits most common use cases

5.4 Private Workspace (Non-Multi-tenant)



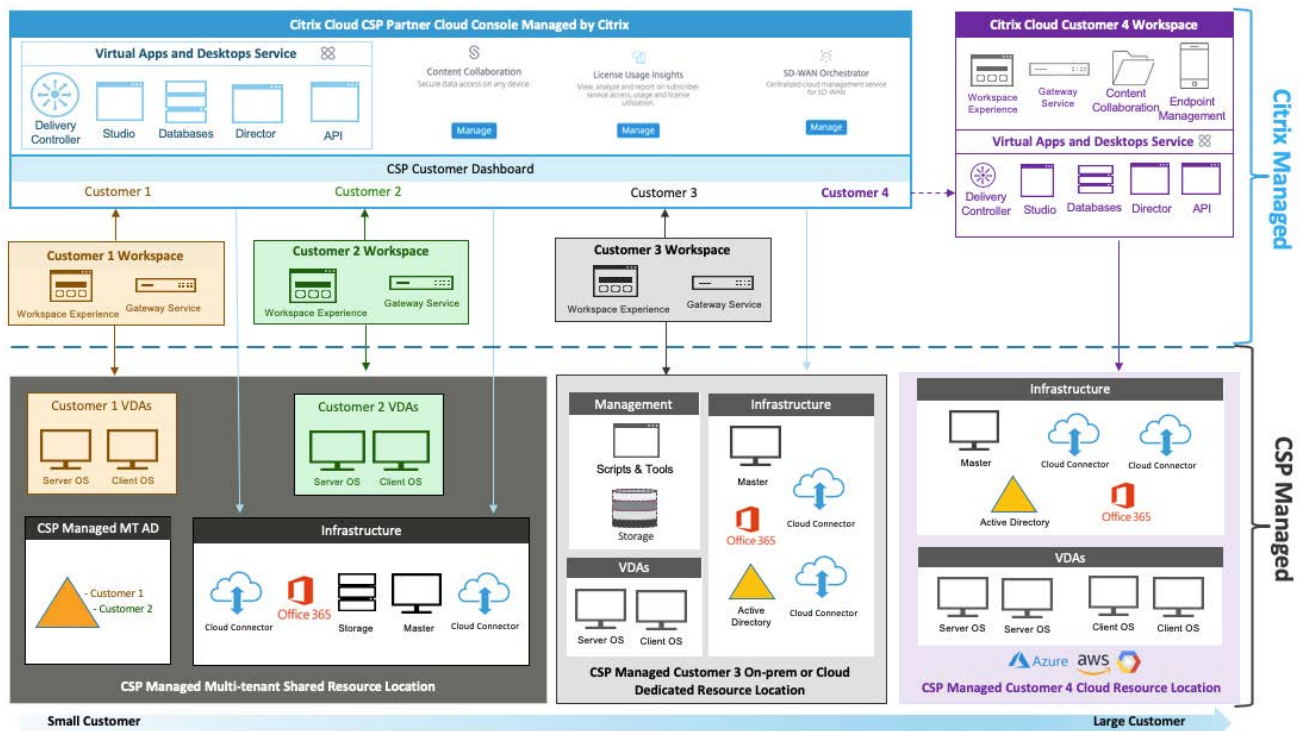
[Private Workspace, showing that the tenant has a fully isolated Workspace and no service instance is shared from the Service Provider's Cloud account]

Some large enterprise customers need the ability to have a private Workspace managed by their Citrix Service Provider for complex applications, and strict security and compliance requirements, the private workspace does not have any shared components with other customers of the same service provider. The service provider will need to be invited by the customer to manage the Cloud environment. This allows for complete isolation, flexibility and control for the customer and service provider. The management and control from the Citrix Service Providers perspective are duplicated with the complete service instance being dedicated to the customer.

The design and deployment for this mode is the same as standalone enterprise accounts on Citrix Cloud except the service provider is invited to connect and administer these accounts, and this is the deployment model available to-date before multi-tenant support became available at the end of 2019. The detailed design, deployment, and best practices of the single tenant private workspace model can be found on [Citrix Tech Zone](#).

5.5 Combination of Different Architecture Models

The different architecture models below are not mutually exclusive, a service provider can apply each model or mixed architectures under their partner cloud account or manage a separate Cloud Account for their large Customer. The Service Provider models are developed to be flexible to meet the needs of their customers, offering solutions for providing a return of investment on shared infrastructure or isolation to solve data sovereignty challenges



[Combined architecture models for customer use cases managed under a single Citrix Service Provider Account]

5.6 Workspace Experience and Authentication

Each customer or tenant has its own workspace, the authentication method used can vary from tenant to tenant if required.

There are several identity providers available to the customers of a Citrix Service Provider.

5.6.1 Active Directory

This is the default provider for a Citrix Service Provider offering the Virtual Apps and Desktops Service and authenticates using Kerberos to a shared or dedicated Active Directory, authenticating with multiple Customer UPN suffixes.

5.6.2 Time-Based One-Time Password

Either single or multi-tenant with or without a token as a secondary factor of authentication that supports the Times Based One-Time Password standard such as Citrix SSO, Google or Microsoft Authenticator.

5.6.3 Azure Active Directory

Citrix Service Providers can leverage Shared or Dedicated Active Directory to control auditing, password policies and account control, with multi-factor authentication. This can be in conjunction with an identity provider such as ADFS, OKTA or Ping, amongst others.

5.6.4 Citrix Gateway

The Citrix Virtual Apps and Desktops Service supports the use per tenant of an on-premises Citrix ADC Gateway and StoreFront that enables multiples of authentication, authorisation and AAA functions

5.6.5 OKTA

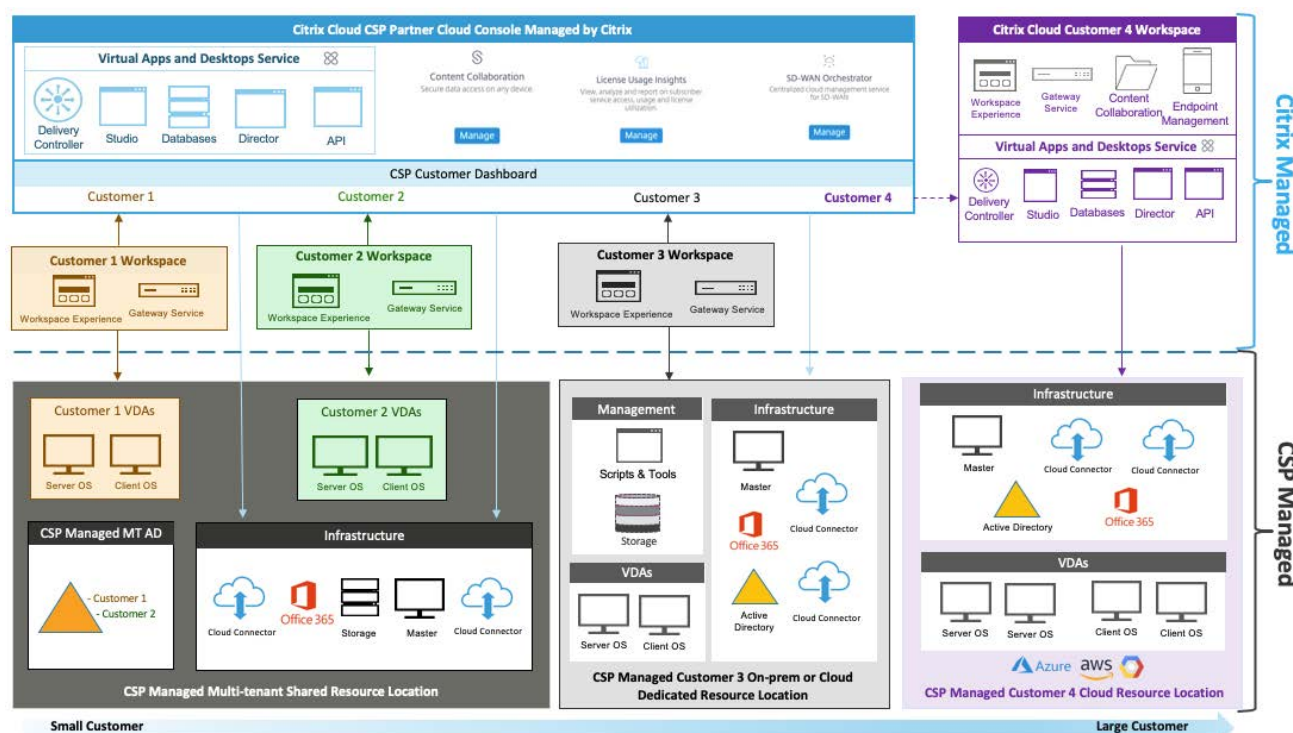
Using a Cloud based identity provider such as OKTA allows CSPs to authenticate Customers providing a common sign-in procedure. This can simplify the management of multiple authentication points for CSPs. At the time of publication OKTA is in Tech Preview

5.6.5 Cloud Federated Authentication Service

This service to enables customers to connect their on-premises FAS deployment to Citrix Cloud. It enables end-users to achieve Single Sign On (SSO) to Citrix Virtual Apps and Desktops resources when using a federated identity provider in Workspace such as Azure Active Directory or OKTA.

6. Deployment Considerations

The Citrix Service Providers Cloud model allows for a wide range of deployment options to best suit the needs of the Service Providers' customers for a wide range of public clouds and hypervisors. Service Providers and their customer can combine these deployment options to provide hybrid cloud migration or multi cloud adoptions.



[Combined deployment options for tenants managed under a single Citrix Service Provider Account]

When ordering the Citrix Virtual Apps and Desktops Service from your chosen distributor, it is important to consider the diverse customer base that can be managed by the Service Provider via Citrix Cloud. If the customer has an existing Citrix Virtual Apps and Desktops service, they cannot be invited to participate as a tenant under the Citrix Service Provider's service instance, however they can be invited to connect and be managed by the CSP. Other customers without an existing service instance can be invited or added to the Citrix Service Provider's instance to either a Shared or Dedicated Resource Location.

In relation to the architecture models, there are two SKU available to CSPs:

Single Tenant SKU – this is the existing SKU that the Citrix Service Provider orders for their Customer, and the entitlement and Service instance are allocated on the Customer Cloud Account. This SKU maps to the single tenant private workspace model.

Multi-Tenant SKU – this is the new SKU with entitlement only delivered to the Citrix Service Provider Partner account that allows managing and distributing licenses between multiple customers.

6.1 Datacenters

Some Service Providers have invested into long term infrastructure and compute to host services or meet stringent compliance requirements, to utilize these existing resources, the suitable option is to have the Resource location deployed in the Citrix Service Provider Datacentre.

Citrix Virtual Apps and Desktops Services supports the main hypervisors available including integration with Machine Creation Service and Provisioning services, automating the delivery and operation of the compute resources.

Service providers normally offer a tired storage option to their customers to ensure that there is distributed performance to allow for their current offering and future expansion.

6.2 Microsoft Azure

Many of our Citrix Service Providers are also Microsoft Cloud Solution Providers. Azure is a public cloud option from Microsoft for Service Providers looking to host workloads in a flexible and elastic way. Citrix Virtual Apps and Desktops has built in support for Azure capabilities allowing for Machine Creation Services Integration. Citrix Autoscale proactively manages the workloads to balance the costs and service levels demanded by the customer, any unused workloads would be reduced during off-peak hours and increased prior to peak hours.

Service providers hosting their customers in Resource Groups in Azure, uses a collection of assets (e.g. Virtual Network, Virtual Machines, Storage accounts) in logical allocations for easy automatic provisioning, monitoring, and access control. They divide the dedicated or shared resource in separate Azure virtual networks, typically the access will be controlled by the Cloud Connectors linking the Azure resource to Citrix Cloud.

For more recommendations regarding Citrix Virtual Apps and Desktops service on Azure see:

<https://www.citrix.com/blogs/2018/06/07/cloud-guidepost-citrix-virtual-apps-and-desktops-service-on-azure-part-2/>

6.3 Amazon Web Services

Amazon Web Services is another public hosting option for Citrix Service Providers looking to host workloads in a flexible and controllable environment. Using an operations cost model to grow their business according to customer demands. Citrix Virtual Apps and Desktops has built in AWS capabilities allowing for Machine Creation Services Integration for on-demand provisioning and Citrix Autoscale to proactively manage the workloads to balance the cost and services levels demanded by the customer. Any unused workloads would be reduced during off-peak hours and increased prior to peak hours.

In Amazon Elastic Compute Cloud, an Availability Group is a collection of assets (e.g. Virtual Network, Virtual Machines, Storage accounts) in logical groups for easy or even automatic provisioning, monitoring, and access control. Resource Groups in EC2 is for grouping related resources that belong to Citrix Virtual Apps and Desktops deployment, as they share a unified resource.

The Virtual Machines used for Citrix Virtual Apps and Desktops workloads in EC2 are typically the T type machines. These Virtual Machines have the best balance for CPU and memory for Citrix Service Providers scaling up and down using Auto Scale to accommodate customer requirements and control the cost. Any unused workloads would be reduced during off-peak hours and increased prior to peak hours.

For more details regarding Citrix Virtual Apps and Desktops on AWS see:

<https://aws.amazon.com/about-aws/whats-new/2019/01/deploy-citrix-virtual-apps-and-desktops-service-on-aws-with-new-quick-start/>.

6.4 Google Cloud

The Google Public Cloud offering for Citrix Virtual Apps and Desktops service allows Service Providers to provision and manage machines within a Project on Google Cloud Platform (GCP), using Machine Creation Services (MCS) to provision workloads and enable lifecycle image management.

The automated provisioning for GCP, working in conjunction with Citrix Autoscale to scale up and down these workloads on demand, at least one Project is needed to run the Citrix Virtual Apps and Desktops Service in conjunction with the Compute Engine API and the “Cloud Resource Manager API. This is all controlled via a GCP Service Account and can be shared between multiple CGP Projects, and the MCS Service will use it to power manage the virtual machines.

For details on setting up a Citrix Virtual Apps and Desktops service resource location on GCP, see:

<https://docs.citrix.com/en-us/citrix-virtual-apps-desktops-service/install-configure/resource-location/google.html>

7. Deployment Steps

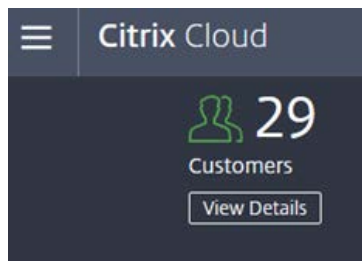
7.1 Onboard a Customer

Customer Dashboard

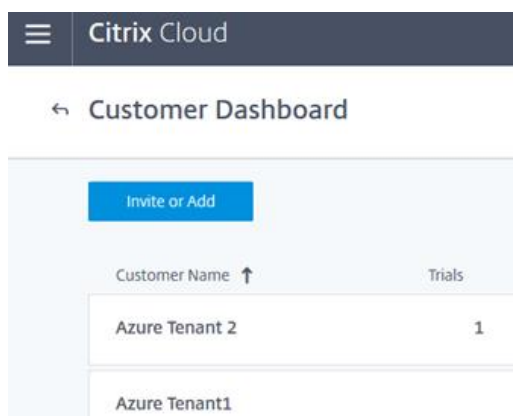
To add a new Customer or invite an existing one to be managed by the Citrix Service Provider, the onboarding process is the same for both multi-tenant and single tenant customers.

7.1.1 Add a new Customer

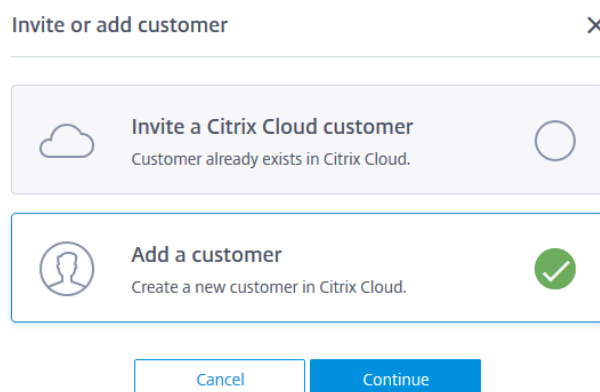
In the Citrix Cloud Dashboard page, select Customers



On the Customer Dashboard you will see all of Citrix Service Provider's managed tenants, to Add a new Customer select Invite or Add:



Select Add and Continue



Complete the onboarding information for the Customer, make sure the email address used here is unique and has not been used for any other Citrix Cloud accounts:

← Add a customer

To add a customer, complete these steps below.

^ Add Customer Information

Enter admin and customer details. (All fields are required)

Admin Details

First Name CSP	Last Name Customer
Business Email Address CSPManagedCustomer@Example.com	

Business Details

This will create a new Customer with a unique Organisation ID (Org ID).



7.1.2 Invite a Customer

To invite an existing Citrix Cloud Customer to be Managed by the Citrix Service Provider, you can select the Invite option.

Citrix Cloud	
← Customer Dashboard	
Invite or Add	
Customer Name ↑	Trials
Azure Tenant 2	1

Select Invite and Continue.

Invite or add customer ×

**Invite a Citrix Cloud customer**
Customer already exists in Citrix Cloud.

Copy the Invite Link and email to the Administrator of the Customer you would like to invite:

Invite Customers

Copy the link below and share it with your customers.

To complete the connection a customer administrator needs to click the link, sign in to their Citrix Cloud account and accept the invitation.

<https://us.cloudburrito.com/invita...>Copy to clipboard

7.2 Enable Virtual Apps and Desktops Service to a New Customer

After a new customer on boarded or an existing customer accepted the invite, the Citrix Service Provider can enable services to that customer (tenant).

7.2.1 Enable Single Tenant (private) Citrix Virtual Apps and Desktops Service

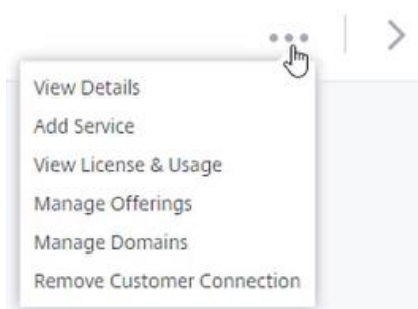
For a new customer in private workspace to have single tenant service, i.e. the customer will have its own instance of Virtual Apps and Desktops service, the CSP needs to make a \$0 order via its distributor and “ship to” the customer’s Citrix Cloud account.

Once the single tenant service instance is enabled for the customer (stocking order fulfilled), “Manage” option will appear inside the Virtual Apps and Desktops service tile, by selecting “Manage” option, the customer’s instance of Studio will load.

7.2.2 Enable Multi-Tenant Citrix Virtual Apps and Desktops Service

Assume the CSP partner already has multi-tenant Virtual Apps and Desktops service entitlement fulfilled on the partner account via \$0 stocking order from the distributor, for a new customer to be managed under the CSP’s multi-tenant service, follow the steps:

- 1) In the Citrix Cloud Dashboard page, select Customers
- 2) On the Customer Dashboard locate the Customer you want to add services to and select the three-dot button and select Add Services



- 3) Select “Continue” next to the Citrix Virtual Apps and Desktops Service



Once the “add service” process is completed in a few minutes, “Manage” option will appear inside the Virtual Apps and Desktops service tile within the tenant’s cloud account, however by selecting “Manage” option, “This instance of the Citrix Virtual Apps and Desktops Service is being managed by your Citrix Service Provider” message will be displayed.



7.3 Configure Multi-tenant Virtual Apps and Desktops Service for the New Customer

This document focuses on the deployment configurations of multi-tenant architecture models, for single tenant Virtual Apps and Desktops Service refer to <https://docs.citrix.com/en-us/citrix-virtual-apps-desktops-service/install-configure.html>.

The following section of multi-tenant deployment uses a hybrid cloud solution as an example to run workloads in an on-premises datacenter.

7.3.1 Deploy a New Resource Location

The resource Location and domain are a 1:1 relationship.

Dedicated Resource Location

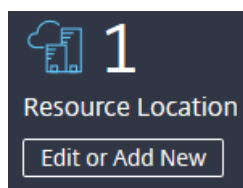
Each time when onboarding a new tenant, a new active directory, resource location, and a pair of cloud connectors need to be setup for the tenant.

Shared Resource Location

The resource location, active directory and cloud connectors only need to be setup when the first tenant of the resource location is onboarded, the subsequent tenants share the same setup except the actual resources to be consumed, e.g. AD OU and VDAs, etc. The Service Provider is responsible to partition the active directory and resources for each tenant with secure isolation.

Process

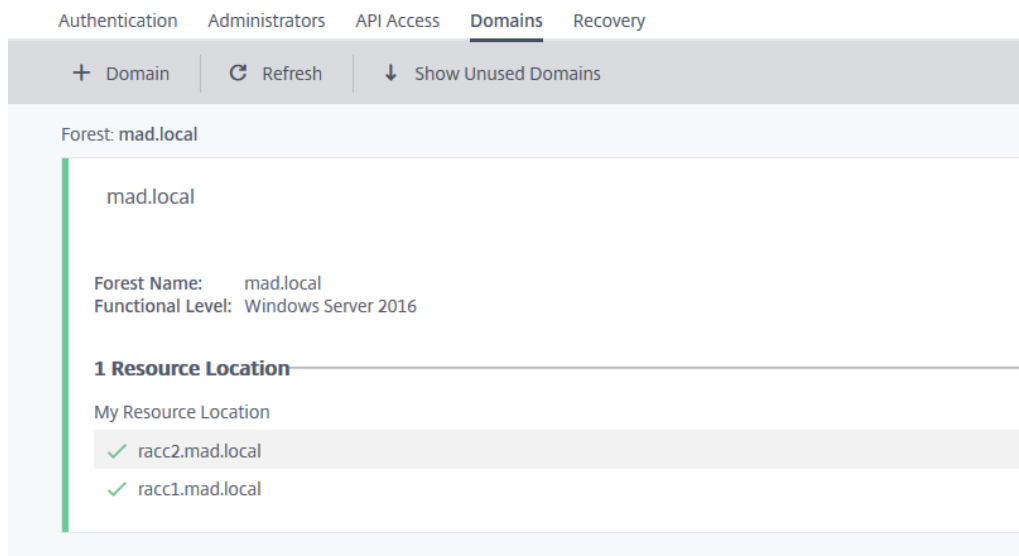
When connected to the Citrix Cloud Console, select Resource Location (Edit or Add New)



Select Add Resource Location, name the Resource location to the multi-tenant nomenclature choose add Cloud Connector, download and install the cloud connector to at least two dedicated Servers, for detailed steps please follow <https://support.citrix.com/article/CTX223580>.

You can view the Active Directory Domain and Cloud Connectors after deployment.

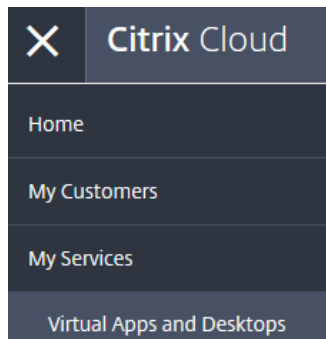
← Identity and Access Management



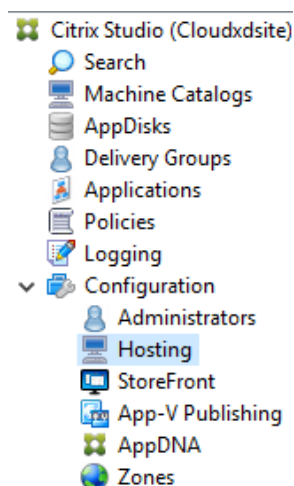
7.3.2 Define Hosting Connection

Since each resource location may be deployed in different cloud infrastructure e.g. Azure, GCP, AWS, on-premises hypervisor etc. a new Hosting Connection to the resources needs to be defined for the new resource location.

Navigate to the hamburger menu at the top left side of the page and choose Citrix Virtual Apps and Desktops.



Select Manage Service, the Citrix Studio will then load, select hosting from the Left-Hand Studio Menu.



Select Add Connection or Resource from the Action pane.

Select Create a new Connection, choose the Connection type and enter the credentials and address for the connection, name the connection using the correct nomenclature.

The screenshot shows the 'Connection' configuration window. The 'Use an existing Connection' option is unselected, and the 'DaaS Pool' dropdown is visible. The 'Create a new Connection' option is selected. The 'Connection type' is set to 'Citrix Hypervisor®'. The 'Connection address' is 'https://10.64.1.10'. The 'User name' is 'root'. The 'Password' field is masked with dots. The 'Zone name' is 'DH-MAD'. The 'Connection name' is 'DH RA MAD Pool'. Below these fields, the 'Create virtual machines using:' section has 'Studio tools (Machine Creation Services)' selected, with a note: 'Select this option when using AppDisks, even if you are using Citrix Provisioning.'

Select the storage location for the Resources.

Select the Network Associated with the new customer.

The screenshot shows the 'Network' configuration window. The 'Name for these resources:' field is 'DH RA On-Premises MAD Network'. Below it, a note states: 'The resources name helps identify this storage and network combination in Studio.' The 'Select one or more networks for the virtual machines to use:' section contains a table with the following rows:

	Name
<input type="checkbox"/>	VLAN 010 Tenant 1
<input type="checkbox"/>	VLAN 020 Tenant 2
<input checked="" type="checkbox"/>	VLAN 030 Tenant 3
<input type="checkbox"/>	VLAN Management Interface
<input type="checkbox"/>	VLAN Storage Interface

Select the scope of the Customer just onboarded, the review the hosting connection and choose finish.

The screenshot shows the 'Scope' selection window. The 'All' option is selected. Below it, the 'All objects' section is expanded, showing a list of resource locations:

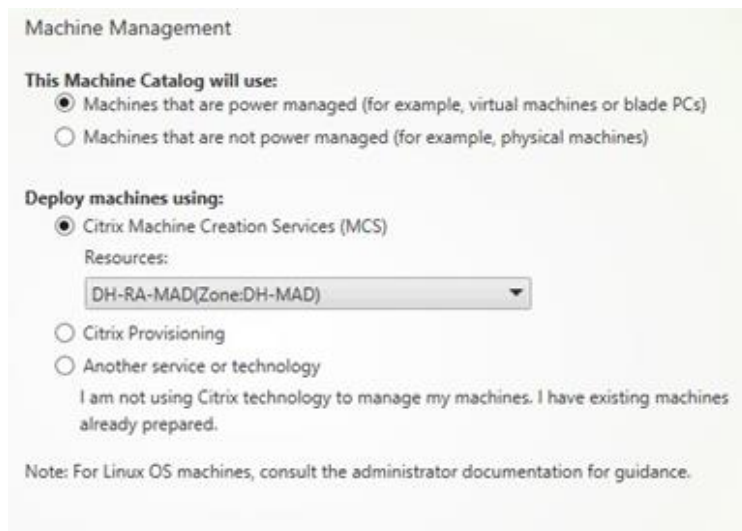
- ☐ _Private Resource Location Tenant1
- ☐ _Private Resource Location Tenant2
- ☐ _Shared Resource Location Tenant3
- ☐ _Shared Resource Location Tenant4
- ☐ _Shared Resource Location Tenant5

7.3.3 Configure Machine Catalogues for the New Customer

In the CSP partner's Citrix Cloud portal page, navigate to Citrix Virtual Apps and Desktops service, and select Manage Service.

From the Citrix Studio, select Machine Catalogues, and Create Machine Catalogues from the Action Pane.

In this example we are using Machines that are created with Machine Creation Services, and are hosted on a hypervisor in the datacenter that is able to control the power state, select the appropriate Resource Location Shared or Single etc. for the corresponding Customer who will be assigned the Machine Catalog, select Next

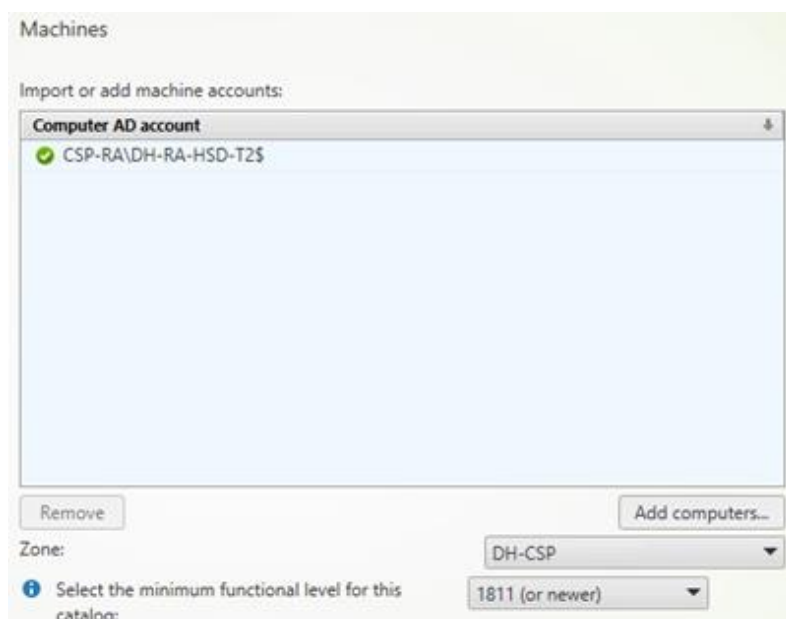


The 'Machine Management' window is used to configure the machine catalog. It contains two main sections: 'This Machine Catalog will use:' and 'Deploy machines using:'. In the first section, the radio button for 'Machines that are power managed (for example, virtual machines or blade PCs)' is selected. In the second section, the radio button for 'Citrix Machine Creation Services (MCS)' is selected. Below this, a dropdown menu for 'Resources' shows 'DH-RA-MAD(Zone:DH-MAD)'. Other options include 'Citrix Provisioning' and 'Another service or technology'. A note at the bottom states: 'Note: For Linux OS machines, consult the administrator documentation for guidance.'

Add the Machines from the Corresponding Active Directory and also the Zone for the Customer.

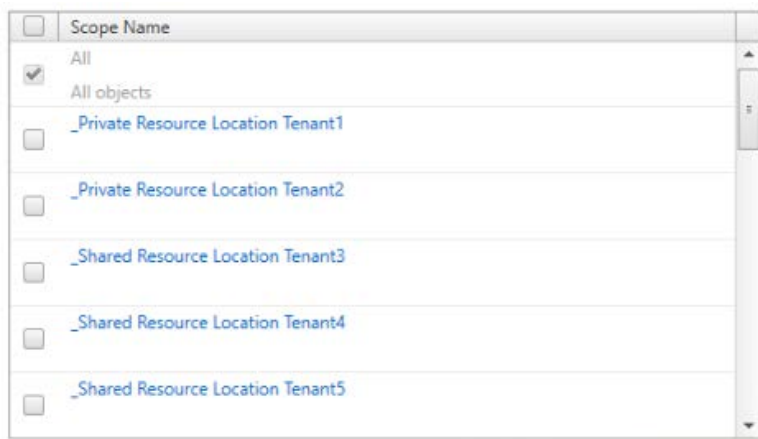
Enter the name of the machines(s) and select OK.

Confirm the Zone and the minimal functional level of the VDA installed on the machines to be added, here we have a VDA that is from version 1811 or newer, select Next.



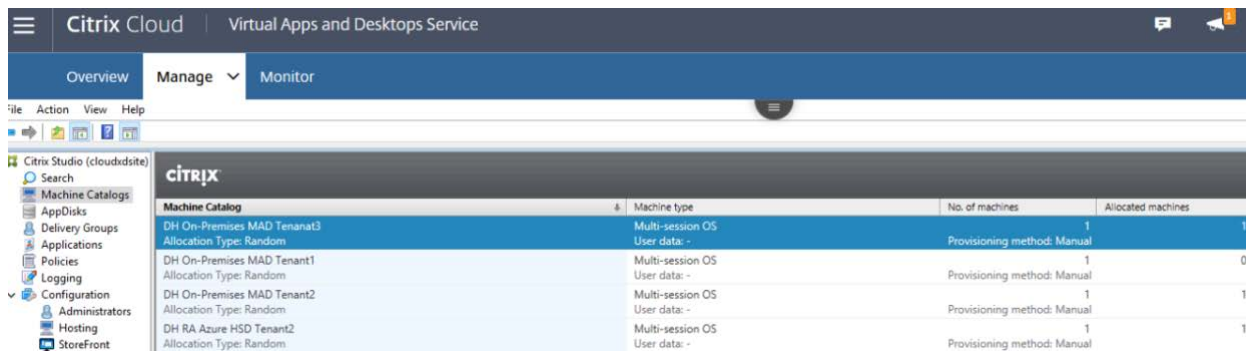
The 'Machines' window is used to import or add machine accounts. It features a list box titled 'Computer AD account' containing the entry 'CSP-RA\DH-RA-HSD-T2\$' with a green checkmark. Below the list box are 'Remove' and 'Add computers...' buttons. At the bottom, there is a 'Zone:' dropdown menu set to 'DH-CSP' and a 'Select the minimum functional level for this catalog:' dropdown menu set to '1811 (or newer)'.

Choose the Scope of the new customer, select Next.

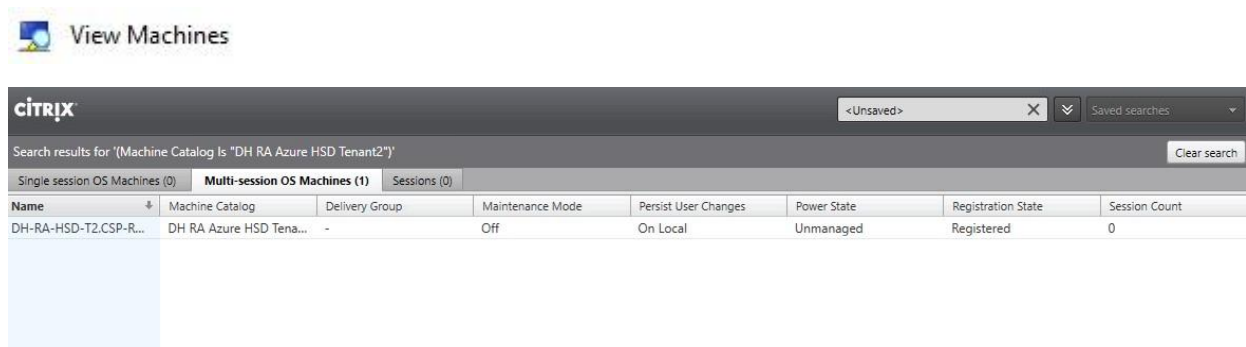


Since machine catalogues are created for specific customer scope, predefined naming convention is necessary in a multi-tenant deployment.

The Machines will then appear in the Machine Catalogue list.



Use the View Machines Search option, to confirm the registration status of the new Machine Catalogue.



7.3.4 Create Delivery Groups for the New Customer

From the Citrix Studio, select Delivery Group, and Create Delivery Group from the Action Pane.

Read the Getting Started information and select Next.

Select a relevant Machine Catalogue that is assigned with the customer's scope, select Next.

Machines

Select a Machine Catalog.

Catalog	Type	Machines
<input type="radio"/> DH On-Premises MAD Tenant1	RDS Manual Random	1
<input checked="" type="radio"/> DH RA Azure HSD Tenant2 Tenant2 Azure located Hosted Shared Des...	RDS Manual Random	1
<input type="radio"/> DH RA HSD Tenant1	RDS Manual Random	1
<input type="radio"/> xcst-tsvda xcst-tsvda	RDS Manual Random	1

Choose the number of machines for this Delivery Group: - +

The recommendation is to leave the management of Users to Citrix Cloud, select Next.

Select Add Applications from a source, usually it is the Start Menu if an application appears there on the corresponding VDA. All applications selected will appear under the same delivery group and be available as Libraries to all subscribers that are later added via Citrix Cloud portal. Separate delivery groups can be created for applications and user groups that need restricted access.

Under the multi-tenant deployment, some delivery groups may contain applications with the same name for different tenants. To avoid confusion to the administrators and clearly define the ownership of these applications, it is recommended to update the application naming to be tenant specific as shown in the example below. Application name for user can remain unchanged.

Application Settings

Studio

Identification

Identify this application.

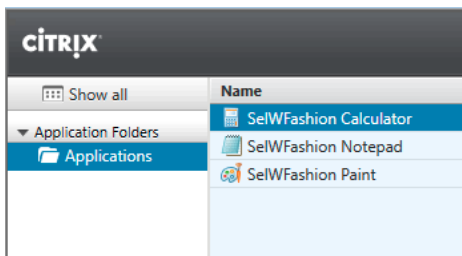
Application name (for user):

Application name (for administrator):

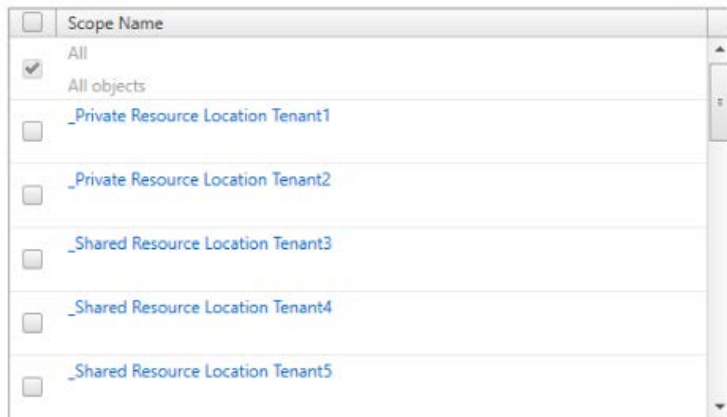
Description and keywords:

This is the description that will be seen by the user. You can also use this field to enter keywords for StoreFront.

OK Cancel



Assign the scope of the customer to the delivery group, and select Next



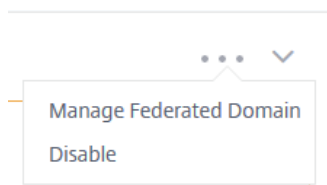
To securely isolate customers in a multi-tenant setup, a delivery group should only be assigned to a specific customer scope. Different customer scopes should not share delivery groups. Predefined naming convention for delivery groups is also necessary in a multi-tenant deployment.

7.4 Configure Federated Domain for the New Customer

For large customers under the single tenant (private workspace) architecture model, this step is not required, as domains and resource locations are configured directly within the customer's cloud account.

For a new customer to be managed under the partner's multi-tenant Virtual Apps and Desktops service deployment and still maintain its own workspace experience, for example to enable the Customers Gateway URL, the customer needs to be federated to the domain configured under the partner account.

Within the partner's Citrix Cloud account, select the Customers domain from the Domains tab in the Identity and access management page, select Manage Federated Domain.



Select the customer(s) to be added to the Domain, this will allow the tenant to use their customized Workspace Configurations.

Add or remove customers to create a federated domain

16 available customers	Add all	2 federated customers	Remove all
<input type="text" value="Search..."/>	<input type="text" value="Q"/>	<input type="text" value="Search..."/>	<input type="text" value="Q"/>
A.Rod Company	+	Citrix Systems Japan KK	×
Cafenatic Store	+	CSPTTest	×
DJ Company	+		
Falcon Cafe	+		

Note: The Federated Domain described here for multi-tenant Virtual Apps and Desktops service is for workspace configuration only, it is not integrated with ADFS or Citrix Federated Authentication Service.

7.5 Subscribe Customer User Groups to Offerings

Under Single Tenant architecture model where each customer has own instance of the service, managing subscribers to libraries is performed directly within the customer's cloud account, for details please refer to the online document <https://docs.citrix.com/en-us/citrix-cloud/citrix-cloud-management/assign-users-to-offerings-using-library.html> .

Under multi-tenant architecture models, subscribing user groups to libraries is performed inside the CSP partner's Citrix Cloud account. The preferred method is to assign well named Active Directory groups to the library resources for easy administration and scalability.

To add users to a published application or desktop offering from either a Shared or Dedicated resource location of the multi-tenant service, locate the Library Offerings from the Citrix Cloud homepage, In the Library offering, select the View Library option, search or find the resource you would like to add users too using the three dot menu, Manage Subscribers, chose from the list of Managed domains and then add the Resource Group.

Manage subscribers for | SelWFFashionBaseAppsDesktop (Applications) X

Step 1: Choose a domain

cms.azr

0 Subscriber(s)

Step 2: Choose a group or user

WFFashion Base AppsDesktop Users| X

1 Item(s) found

G

SelWFFashion Base AppsDesktop Users

✓

TypeSubscriberStatus

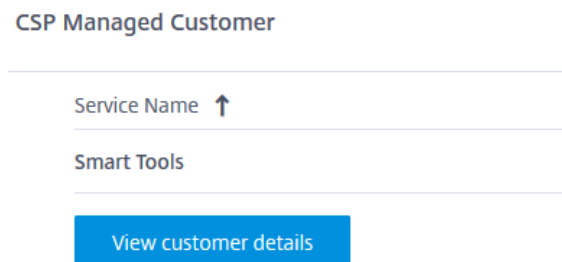
To add a **Group** or **User** to this offering first select a domain or Azure account.

7.6 Configure Tenant Workspace

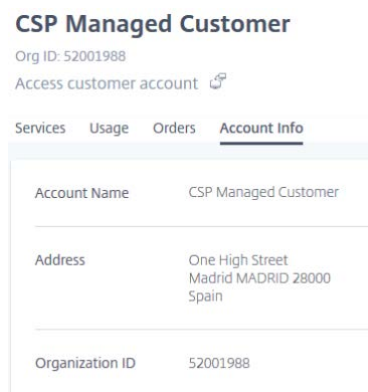
The CSP multi-tenant Virtual Apps and Desktops service allows each tenant to maintain its own Workspace Experience.

To change the Workspace for a customer from the Citrix Cloud Dashboard page, select Customers, view Details.

Select a customer and Expand using the Arrow, select View Customer Details.

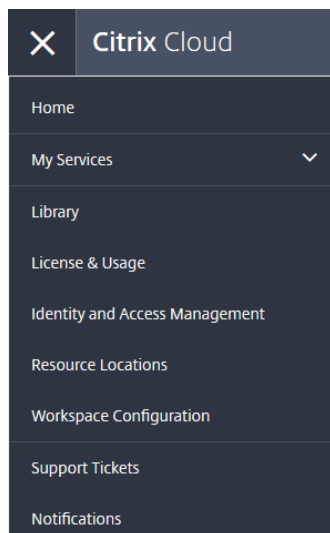


Select Access Customer Account (there is also an alternative way to access the customer's account via Change Customer)



Confirm that you are leaving the Citrix Service Provider's Account to enter the Customer Account and select Continue.

After entering the tenant's Citrix Cloud account, navigate to the hamburger menu and choose, Workspace configuration:



7.6.1 Access URL

Under the Access tab, the Customers Gateway URL can be customized. Edit the URL and select Save.

Workspace Configuration

Access Authentication Customize Service Integrations Sites

Workspace URL: https:// .cloud.com

☒ I understand that changes to my Workspace URL can take up to 10 minutes and will cause an outage to my subscribers.
The new Workspace URL will need to be distributed to your subscribers. You will also need to manually update Citrix Workspace apps to direct t

7.6.2 Authentication

In the Authentication tab, specify the Authentication method for the customer:

Workspace Configuration

Access Authentication Customize Service Integrations Sites

Workspace Authentication

Select how subscribers will authenticate to sign in to their workspace.

☒ Active Directory

☐ Active Directory + Token

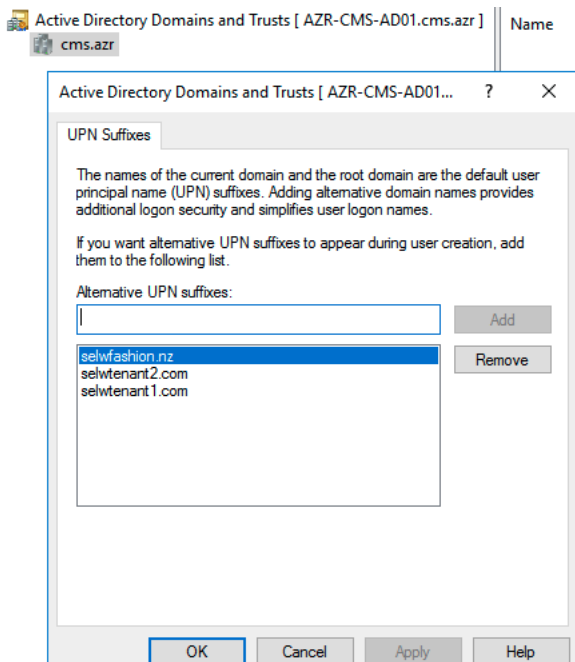
☐ Azure Active Directory

☐ Okta

☐ Citrix Gateway

If Active Directory Authentication is used and the tenant is configured within a shared resource location, i.e. the tenant user accounts and groups reside within an OU of the hosted multi-tenant Active Directory, the users' UPN suffix which is normally the customer's own domain that differs from the AD system domain, e.g.

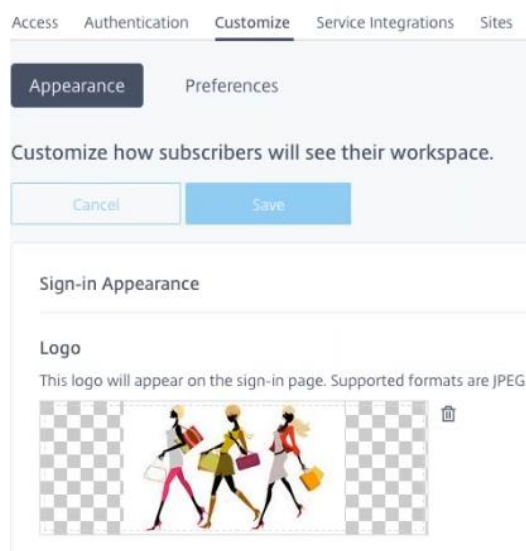
customer domain selwfashion.nz in the example below vs cms.azr system domain of the hosting AD; for the user's UPN domain to be recognized and authenticate through the custom Workspace URL, the UPN suffix needs to be added to the hosting Active Directory at root level.



7.6.3 Appearance

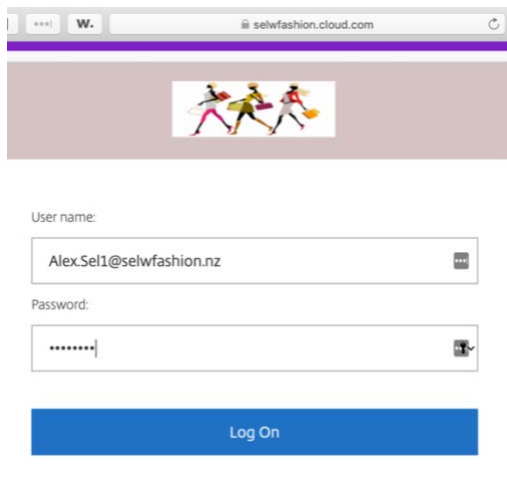
Customized branding and appearance often help achieve great result for end user experience. From Customize tab, configure the customer logo and preferences.

Workspace Configuration



7.7 User Login to Workspace

When the users of a customer login to the Workspace via the customized URL, e.g. <https://selwfashion.cloud.com>, same set of credentials of UPN and password (e.g. email address and password that match their Office 365 accounts) will be used.



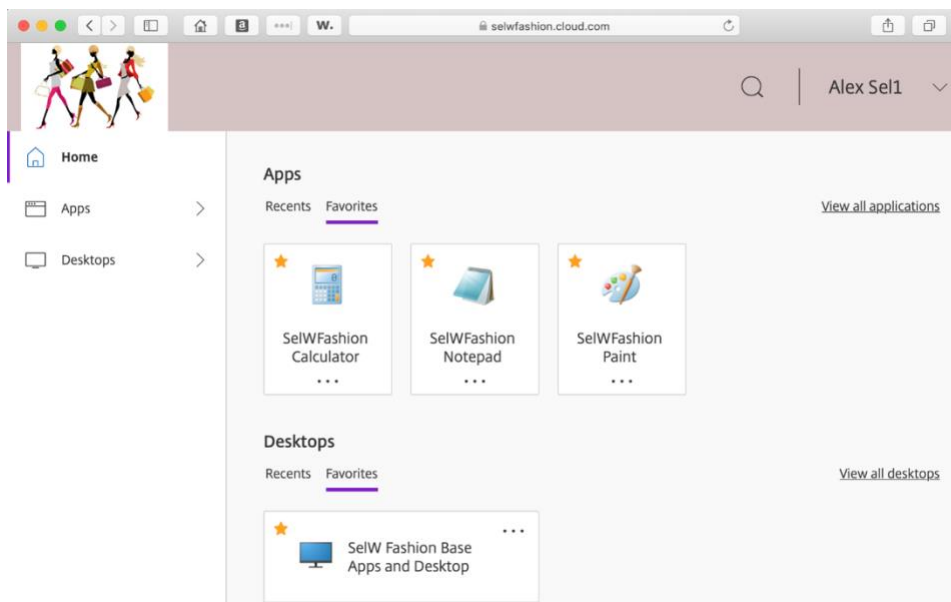
W. selwfashion.cloud.com

User name:
Alex.Sel1@selwfashion.nz

Password:

Log On

After logging on the user's workspace would look similar as below.

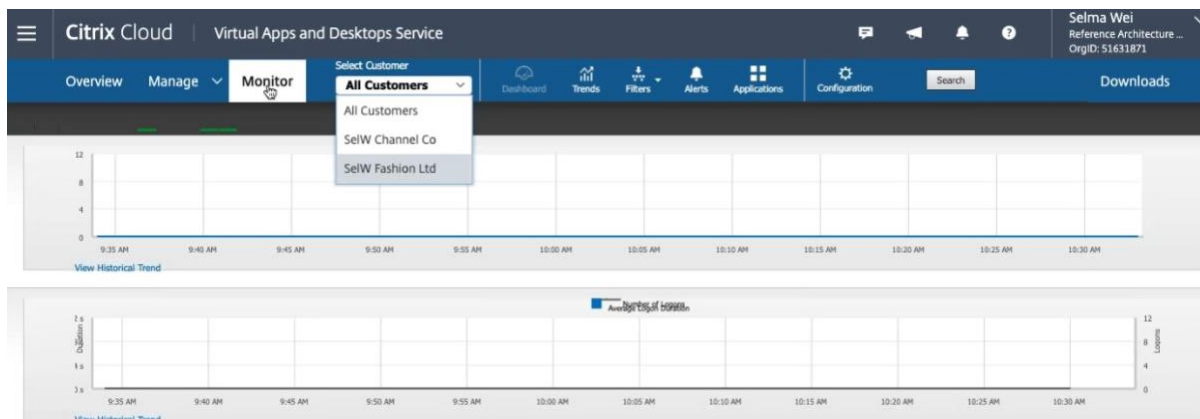


8. Performance and Monitoring

The Citrix Virtual Apps and Desktops Service allows Citrix Service Providers to control and monitor the workloads centrally in the Cloud Console, this lowers the cost and administration effort of the management and allows the operations team to deliver greater uptime.

8.1 Director

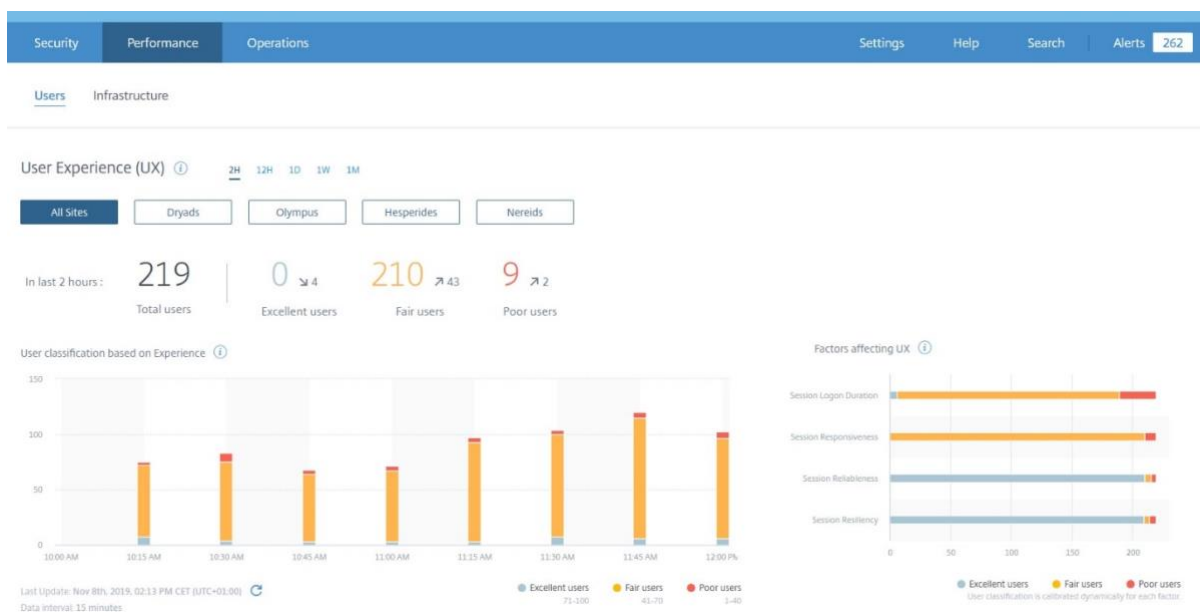
The Citrix Service Provider admins has the ability to manage their multi-tenant Shared and Dedicated Resource location Customers using a single Monitoring console, the CSP admin can chose to view an overview of all resources or drill down to a specific Customer. The Service provider can also set Role Based Access Control permissions for its team remembers to manage specific customer scope or perform a subset of functions.



Single tenants in their private workspace with own instance of Citrix Virtual Apps and Desktops Service, their Monitoring console is dedicated. A Citrix Service Provider with administrator rights will need login to the customer's cloud account to access and manage through this console.

8.2 Citrix Analytics Service

The Analytics service included in the Citrix Service Providers Workspace collects data across the hosting network, users, files and endpoints. A Service provider can centrally manage the insights to handle security threats, monitor service performance and optimise and improve their offering.



9. Appendix

Common Abbreviations

ADC	Application Delivery Controller
AWS	Amazon Web Services
BYOD	Bring your own Device
CCC	Citrix Cloud Connector
CEM	Citrix Endpoint Management
CVAD	Citrix Virtual Apps and Desktops
CWS	Citrix Workspace Service
EFSS	Enterprise File Sync and Sharing
EMM	Enterprise Mobility Management
HSD	Hosted Shared Desktops
LUI	License usage insights
MAM	Mobile Application Management
MDM	Mobile Device Management
RBAC	Role Based Access Control
SDN	Software Defined Networking
SD-WAN	Software Defined WAN
VDA	Virtual Delivery Agent
VDI	Virtual Delivery Infrastructure
VM	Virtual Machine

10. References

Supported Hypervisors for Virtual Desktops (XenDesktop) and Provisioning Services

<https://support.citrix.com/article/CTX131239>

Supported Host Connection Resources

<https://docs.citrix.com/en-us/citrix-virtual-apps-desktops-service/system-requirements.html>