Citrix IRAP Supplemental Guide

Common Deployment Guidance

The Citrix website includes significant information on deploying and configuring Citrix Cloud and the services that run under that cloud infrastructure. The vast majority of the material in the commercial guidance is applicable to all configurations and this information is not reinvented for security standards. Certification specific guidance is listed in the documentation sections that follow.

"Citrix Cloud" is the foundation cloud infrastructure of many Citrix services including

- Citrix Virtual Apps and Desktops Service (XenApp and XenDesktop)
- Citrix Endpoint Management Service (XenMobile)
- Content Collaboration (ShareFile)
- Citrix Gateway Service
- Workspace Service

The Citrix Cloud platform and all of the services except Content Collaboration run on Microsoft Azure clouds. Citrix Content Collaboration (ShareFile) runs under Amazon Web Services. Each service may be in-scope or out of scope for the specific security standard.

Citrix Cloud Regions

During enrollment, customer administrators select their organization's "region". This selection is a "once" configuration and cannot be changed once enrolled. Full documentation on region selection is in Citrix documentation on Citrix Cloud Regions. There are Citrix Cloud regions in the United States, European Union and Australia as well as Citrix Cloud Government for the US Public Sector.

IRAP customers would normally host their region as Australia.

There is a 1:1 relationship of Citrix Cloud regions to Azure regions, with the Citrix set being a subset of the Azure portfolio. While "Azure" is in focus, there are cases where Citrix Cloud and Citrix products use services from other clouds. For example, Citrix Content Collaboration (ShareFile) is primarily hosted in Amazon Web Services. Citrix Gateway Service for another example runs in more than 14 points of presence around the world, a larger set of Azure locations than which host Citrix Cloud.

Commercial Deployment Guidance

A number of documents exist on Citrix.com showing common architecture and usage of Citrix Cloud. These provide a good introduction to the software and implementation common in commercial usage.

- Secure Deployment Guide For The Citrix Cloud Platform
- Citrix Cloud Government Secure Deployment Guide
- How Do I Deploy Citrix Virtual Apps and Desktops (includes video demo)
- Connect Azure Active Directory to Citrix Cloud
- Cloud Connector Internet connectivity requirements
- Credentials handling and network configuration of Workspace Service and StoreFront
- Citrix Cloud Connector Technical Details
- Migrate VPX To Gateway Service For HDX Proxy.html

The above provide an excellent introduction, including show and tell videos of customer-view, cloud setup and system configuration. The security standard specific guidance is an addendum of the standard configuration guidance, calling out the configuration expectations specific to each security standard.

Global configuration norms

Citrix strives to keep clouds consistent in construction and consistent in content. Security standards drive many requirements and some of the security controls built for “one cloud”, effect and benefit “all clouds”.

TLS 1.2 required throughout Citrix Cloud

In March 2019, Citrix depreciated the use of TLS 1.0 and TLS 1.1 across all instances of Citrix Cloud. This change was required for compliance with execution in Citrix Cloud Gov. A positive security change and supporting the goals of many security standards, TLS 1.0 and TLS 1.1 have been disabled and this change has been implemented globally. For more information, consult CTX247067.

Citrix Responsibility

Citrix Cloud and services configured to require TLS 1.2 or above and utilize FIPS/NIST approved cryptographic algorithms.

Customer Responsibility

Citrix Receiver clients and Workspace App are both capable of communicating at TLS 1.2. This is “standard” for all recent versions of Citrix Receiver and all versions of the newer client, Workspace App. Older Thin Client machines may require update to communicate at TLS 1.2 and customers need to ensure that their Thin Client inventory support TLS 1.2.

FIPS 140-2 Compliance

All Windows servers in Citrix Cloud are configured in FIPS Mode. As with the disable of TLS 1.0 and TLS 1.1, use of FIPS cryptography is a positive security enhancement for all Citrix Cloud regions, and this change was implemented globally during 2019. Note that it was rolled out to Citrix Cloud without customer impact and without a KB article needed as with disabling of TLS 1.0 and TLS 1.1.

Password splitting

User logon to cloud Workspace Service is accomplished using credentials provided by user, this page describes how the user password is encrypted on transmission to hosted virtual desktop agent for SSO use during logon to the hosted system, with the key traveling through cloud and encrypted credentials traveling via Receiver to the VDA, and then reassembled on the VDA.
https://docs.citrix.com/en-us/citrix-virtual-apps-desktops-service/secure.html

Data routing and storage caveats

Data held by Citrix Virtual Apps and Desktops is restricted to information needed for application and desktop publishing. The CVAD service needs to know

- Names of applications
- Icons for applications
- List of usernames and AD groups to which applications are published

This information does not include vision to the application executables which are executed, nor the data held and processed by those applications on customer hosted virtual machines. The end user computer connects to the Virtual Desktop Agent (VDA) and execution of the application or desktop occurs in customer-managed systems.

In configurations using Citrix Gateway for remote access, data travels from end user computer to the Gateway, and on to the VDA. For cloud hosted Gateway (Gateway service), the data travels through the Gateway Service and to VDA execution space using Cloud Connector. This data is encrypted through the cloud in transit using TLS. With Gateway Service this data can also be TLS encrypted on the customer resource location. See “Rendezvous” later in this document and note that this function defaults “off” and commonly should be enabled by customer administrators in most configurations.

Citrix Gateway Service, user connection to hosted execution is routed through the Gateway Service in each region. If a region is down, this data can is routed to through other regions to keep the user session up. The Gateway Service also has points of presence across many more Azure clouds than which host the full Citrix Cloud, enhancing resiliency, reducing latency and improving user data throughput. Data traveling from user to customer resource location is TLS encrypted.

The StoreFront or Workspace Service are websites providing a list of available for remote execution. These have only limited information applications/desktops are available for launch. This data is “less sensitive” compared to the application data which is processed by the application. The application and Desktop are executed on customer held virtual machines, with the screen and keyboard activity directed to the end user machine using virtual desktop agent on the host computers and corresponding Receiver / Workspace App on the end user machine.

Customer Active Directory

While Citrix has no vision to the application data on customer resource location, Citrix does need access to user and group data from Active Directory to support brokering and publishing. Connectors provide this data, allowing the infrastructure of Citrix Cloud and the Desktops and Applications Service, to query user information in customer resource location.

Logging

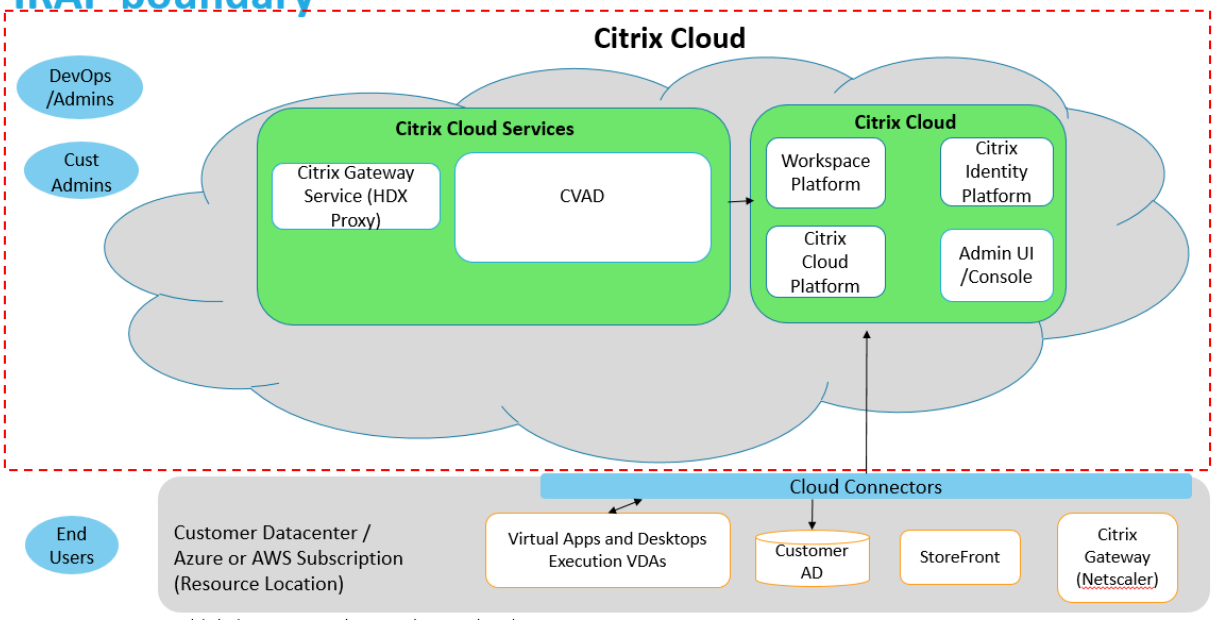
Citrix Cloud logging data is held primarily in Splunk. This includes information on application publishing, usage and failure events. Data logged includes information needed to support and deliver Citrix Cloud. It does not include customer application data.

Data Sovereignty

Publishing and log data may be transferred between regions to assist disaster recovery.

IRAP Scope and Deployment Guidance

IRAP Scope



Boundary legend

- Red dashed area represents the IRAP authorization boundary
- HDX Proxy – formerly referred to as NGS Gateway service PoP (there are currently 19 PoPs globally)
- Admin UI box represents a web console for customer admins to manage apps/desktops delivered to their users
- Cloud Connectors are out of boundary
- Workspace Environment Management (WEM) is not in scope, customers may use at their discretion
- Gateway (ICA Proxy) can be hosted by Citrix as Citrix Gateway Service or on customer premises as Citrix Gateway
- Application and Desktop publishing website can be on customer premises as StoreFront or managed by Citrix as Workspace Service

Azure Active Directory

Citrix Workspace is able to utilize Azure Active Directory for user authentication. Customers considering using Azure Active Directory with PROTECTED workloads should consult the ACSC CONSUMER GUIDE – Microsoft Azure at PROTECTED for implementation guidance.

Printing

Printing best practices, please consult https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/printing/printing-best-practices.html

Banners

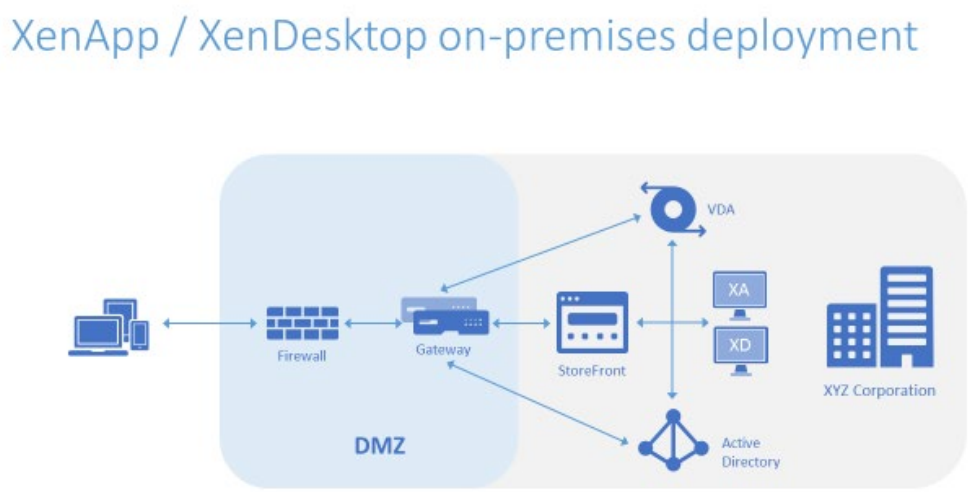
Citrix StoreFront and Workspace, Citrix services a diverse range of customers and Citrix is not able to comply directly with ISM control 0408 (Systems have a logon banner that requires users to acknowledge and accept their security responsibilities before access is granted). The logon system exists for many customers, not just for those needing IRAP. Citrix recommends that customers ensure that their personnel with access to the Workspace portal are educated on their security responsibilities.

Windows computer logon, customers control the virtual desktop agent computers (hosted systems) and customers can themselves include logon banners during Windows computer logon.

Citrix Gateway via Cloud or on premises

As described in the IRAP Scope diagram, the IRAP configuration permits both cloud Citrix Gateway Service (Gateway in cloud) as well as Citrix Gateway (Gateway on premises). This gives the customer administrator considerable flexibility. Gateway configuration is a per-resource location setting.

Citrix Gateway (on premises)

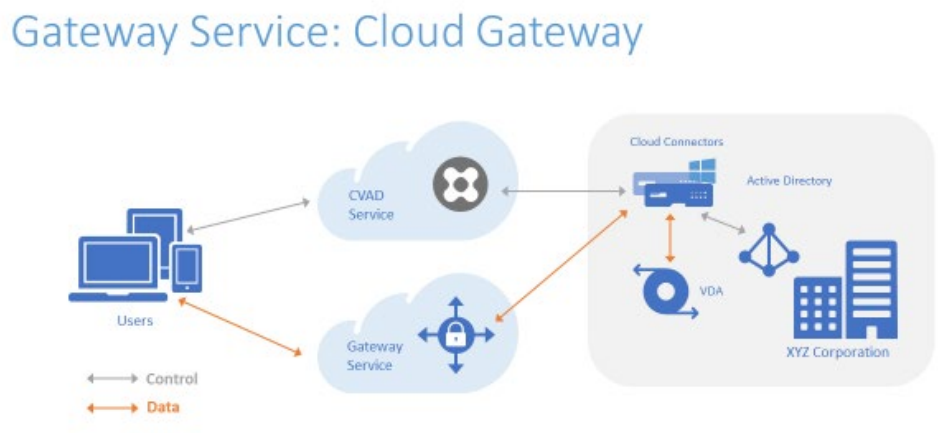


Cryptography with on premises gateway

In all scenarios, the ICA data connection from end user computers to the Citrix Gateway is delivered via TLS. This requires the administrator to install a (one) TLS server certificate onto the Gateway and this is standard practice in gateway configuration.

With an on premises gateway, the customer's resource location internal ICA data traffic is encrypted with either Basic, SecureICA or TLS. The best of these is TLS. Setting up TLS on the internal network requires adding TLS certificates to the VDA "hosts" - this is a customer administrators' required step for the most secure configurations. Details on how to set up TLS in this configuration can be found in Citrix Virtual Apps and Desktops FIPS Compliance documents at https://citrix.com/trust.

Citrix Gateway Service (cloud)

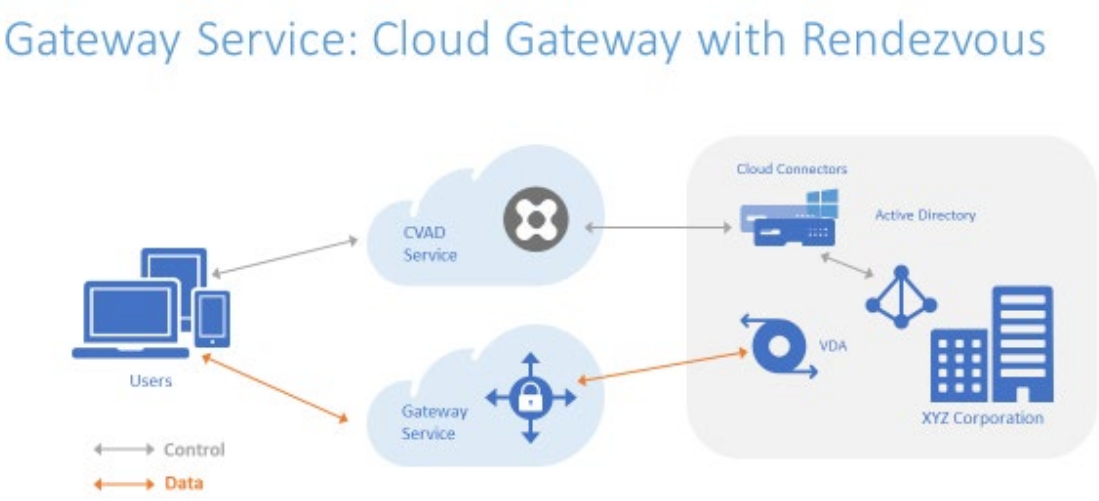


Rendezvous and security advantages of Cloud Gateway

The cloud gateway has capability for rendezvous connection of VDA to Gateway. In this configuration, the TLS "host" is changed from the VDA to the Gateway. Instead of the Gateway establishing a TLS connection with the VDA as in the historic Citrix Apps and Desktop configurations, the VDA establishes a TLS connection to the Gateway. The end user establishes a TLS connection with the Gateway and the VDA rendezvous as the same gateway. Using connection tickets, the Gateway connects the outside to inside for delivery of the HDX/ICA data.

Rendezvous defaults "off" and should be turned "on" for all normal configurations (Cloud Gateway configuration).

Since only the Gateway Service requires TLS certificates, the on-premises administrator burden of installing and maintaining per-VDA TLS certificates is avoided.



Workspace Service OR StoreFront

IRAP deployment guidance permits administrator option for using either StoreFront inside customer resource location, or Workspace Service in cloud. Using the cloud service moves more of the customer infrastructure into Citrix managed cloud space and is the preferred configuration for most cloud implementations. Workspace Service also enables single user view integration with additional services such as including the Citrix Content Collaboration Service.

Since both options are included in scope, the administrator can choose the correct StoreFront vs. Workspace Service configuration for their environment

Closing

IRAP deployments in Citrix Cloud are primarily consistent in implementation to the standard Citrix commercial guidance. The region for Australia workloads should be the Citrix Cloud region in Australia. Administrators have options for configuring their environment for either cloud Workspace Service or on a customer resource located StoreFront. Administrators also have option to use cloud hosted Gateway Service or a customer resource located Gateway.