Security Basics

Security Basics

Sometimes users reside behind corporate networks that have strict network access policies. Connection issues can arise if certain domains are being blocked. To avoid this, administrators ensure that the Network Configuration Requirements for their deployment architecture are met.

Anti-virus Software on Frame

Frame images do not include anti-virus or anti-spyware tools. Administrators are responsible for installing and configuring their own choice of AV/AS tools. For non-persistent Frame accounts, systems are stateless. As long as administrators are diligent about their work in the Sandbox servers, “exposed” production systems that are infected will be reverted on reboot. In the case where Frame provides the initial base image (public cloud infrastructure only), Frame ensures that all base images are scanned before customers use them to create their Frame accounts.

While many anti-virus software packages will work on Frame, due to the large number of anti-virus packages, and the possible complexity of configuration, interoperability is not guaranteed. Anti-virus software that prevents components of the Frame service from executing may cause loss of functionality within a Frame session, up to and including a complete inability to connect to sessions. Prior to installing an anti-virus package, a backup of your account's Sandbox should be taken in the event that issues occur. Since most Frame customers use stateless systems, all anti-virus database updates will download each time a production instance is started. This can be avoided either by maintaining the Sandbox image (updating the Sandbox and publishing to production instances regularly) or using Persistent Desktops.

Exclusion Rules

Any anti-virus software used on Frame-managed workloads must be configured to allow the following directories and associated sub-directories:

- `C:\\ProgramData\\Nutanix\\Frame\\`

> Contains libraries and utilities for Frame Service, Server, and logs (FGA 8.x).

- `C:\\Program Files\\Nutanix\\Frame\\`

  > “Contains Frame Service executables which provide communication to the Frame Platform for orchestration (FGA 8.x).

- `C:\\Program Files\\OFS\\`

  > “Contains Frame file system driver and control application.

- `C:\\OFS\\`

  > “Contains Frame file system driver components.

If you intend to use Enterprise Profiles, please allow the following folders and files:

Folders:

- `C:\\Program Files\\ProfileUnity\\` and all subfolders
- `C:\\Windows\\Temp\\ProfileUnity\\`
- `C:\\FADIA-T\\`
- `C:\\ProfileDiskMounts\\`

Files:

- `C:\\Windows\\System32\\drivers\\Cbfltfs3.sys`
- `C:\\Windows\\System32\\drivers\\Cbfltfs4.sys`
- `C:\\Windows\\System32\\drivers\\Cbreg.sys`
- `C:\\Windows\\System32\\drivers\\cbfsfilter2017.sys`
- `C:\\Windows\\System32\\drivers\\cbfsregistry2017.sys`
- `C:\\Windows\\System32\\drivers\\cbregistry20.sys`
- `C:\\Windows\\System32\\OFS_x64.dll`
- `C:\\Windows\\System32\\drivers\\OFS.sys`

> Please ensure that anti-virus "Tamper protection" is disabled during the publishing process.

>

During a Sandbox publish, Frame will clone the Sandbox disk image to create production workload VMs. If the Frame account is configured for domain-joined instances, then the Sandbox disk image is cloned and the cloned Sandbox disk image is used to create a new VM ("Generalized Sandbox VM"). This Generalized Sandbox VM is powered on and generalized using sysprep before creating the domain-joined production workload VMs. Consult with your anti-virus solution provider to determine if your anti-virus solution must be configured to account for either of the two Frame publishing workflows.

SSL Break and Inspect

Frame Remoting Protocol (FRP) is an H.264-based bi-directional communication protocol between the end user and the workload VM. This communication consists audio/video streamed from the workload VM to the user's endpoint and keyboard/mouse/peripheral input from the end user's endpoint to the workload VM. With FRP 7.0, the protocol uses Secure WebSocket (WSS) over Transport Layer Security (TLS). With FRP 8.0, the protocol builds on WebRTC, a real-time communication protocol using UDP and Datagram Transport Layer Security (DTLS). Customers can use out-of-band monitoring solutions to monitor these FRP streams; however, inline or in-band solutions that break and inspect FRP traffic are not supported as they either prevent FRP from functioning or introduce latency that degrades the end user experience. From the end user's perspective, SSL break/inspect can result in sluggish desktop behavior, the display video skipping frames, and abrupt disconnects of the video stream while in session.

From a security perspective, the FRP streams does not add an inherent risk as it is a video/audio stream from workload to endpoint. If clipboard synchronization, file upload/downloads, microphone input, and remote printing are disabled for the users' Frame sessions, then the only data being sent to the user endpoint is the audio/video display of the desktop and keyboard/mouse events from the user to the workload VM. Breaking and inspecting the traffic will only reveal raw data streams (H.264 encoded display pixels) and keyboard/mouse events.

Frame orchestration and brokering management communication between Frame Guest Agent (FGA) on the workloads and Frame Platform as well as from Prism Central/Element to Frame Platform originates within the customer's private network from the workloads and Cloud Connector Appliance (CCA) VMs as HTTPS requests, switching over to Secure WebSocket over TCP or WebRTC over UDP for bidirectional communication. FGA on the workload VMs and CCAs can be configured to support outbound HTTPS/Secure WebSocket proxy servers.

Revision #5
Created 1 October 2025 04:55:08
Updated 19 January 2026 14:36:46 by Dominik Conrad