JUMP DESKTOP FOR TEAMS

WHITE PAPER

EXECUTIVE SUMMARY

WHAT IS JUMP DESKTOP FOR TEAMS?

What is Jump Desktop for Teams?

Jump Desktop for Teams is an enterprise-grade cloud remote desktop infrastructure, based on Jump Desktop, that enables your team to securely connect from their computers and mobile devices to any computer anywhere in the world.

No programming or additional infrastructure like VPNs or gateways are required. High level security: encryption, access control – including Single Sign On – are all built-in to Jump Desktop for Teams.

WHY JUMP DESKTOP FOR TEAMS?

Secure remote access for everyone

Secure remote access – where connections to enterprise computers unavoidably traverse public networks – has always been important to many enterprises. But now, at a time when working from home has become the new normal, IT managers face the challenge of enabling *all* their users to remotely access enterprise computers while maintaining the same level of security enforced for local users.

Full authentication and authorization

Jump Desktop for Teams meets this challenge by allowing users remote access only to the computers to which they have been authorized to connect, and only after authentication and authorization, while at the same time preventing malicious actors from hijacking connections over the public network for their own purposes.

Complete protection for enterprise assets

Enterprise assets are fully protected:

- Jump Desktop for Teams connections are encrypted end-to-end.
- IT managers can grant or revoke user access to specific computers or to groups of computers at any time.
- Once users initiate a connection to the enterprise computers, their access to other enterprise assets is controlled by the same access controls enforced for local users (Active Directory, LDAP, *etc*.).
- Cloud-based logging provides detailed forensic information for compliance requirements.

Jump Desktop's Cloudless Fluid feature enables even organizations whose networks are not connected to the internet (because of unique security requirements) to use Jump Desktop for Teams.

Jump Desktop for Teams gives your users the remote access they need. It's easy to install and configure, and it's also easy to try out with a no-risk, no obligation, no-cost free trial.

What is Jump Desktop for Teams?

What is Jump Desktop for Teams?

Jump Desktop for Teams is an enterprise grade cloud remote desktop infrastructure, based on Jump Desktop that enables your team to securely connect from their computers and mobile devices to any computer anywhere in the world.

Jump Desktop for Teams is based on Jump Desktop, a proven remote access application used by hundreds of enterprises and thousands of users worldwide. Jump Desktop is built on Web Real-Time Communication (WebRTC), a modern, industry standard open-source project supported by Apple, Google, and Microsoft, among other leading companies. WebRTC specifications have been published by the World Wide Web Consortium (W3C) and the Internet Engineering Task Force (IETF).

With Jump Desktop for Teams, IT managers can quickly and easily give everyone on their team secure remote desktop access from anywhere in the world. No programming or additional infrastructure like VPNs or gateways are required: security, end-to-end encryption, and full access control – including Single Sign On – and are built-in to Jump Desktop for Teams.

Why Jump Desktop for Teams?

Remote access – where connections to enterprise computers unavoidably traverse public networks – has always been important to some enterprises. But now, at a time when working from home has become the new normal, IT managers face the challenge of enabling *all* their users to remotely access enterprise computers while maintaining the same level of security implemented for local users.

Securing remote access over public networks

Jump Desktop for Teams meets this challenge by providing authorized users with full access while at the same time preventing malicious actors from hijacking connections over the public network for their own purposes.

Jump Desktop for Teams provides administrators with full control over their users' access to the enterprise computing infrastructure. Access is granted only after authentication and authorization, connections are encrypted end-to-end and mediated by the Jump Desktop Cloud Infrastructure and, if a direct connection cannot be established, by either the worldwide network of stateless Jump Desktop Relay Server or the enterprise's private on-premises Relay Servers.

Administrators can monitor the devices a user is signed into and remotely log users off a computer, can grant or revoke users access to specific computers or to groups of computers, configure a maximum session duration after which a user is signed off and must sign in and authenticate again, enforce two-factor authentication for team members, and require direct VPN only connections.

Cloud-based logging provides detailed forensic information for compliance requirements.

Note: Once users gain access to the enterprise computers, their access to other enterprise assets is controlled by the same access controls implemented for local users (Microsoft Active Directory, LDAP, *etc*.).

Jump Desktop Overview

Jump Desktop for Teams Infrastructure

Jump Desktop for Teams connections are encrypted end-to-end, and are mediated by the AWS-based Jump Desktop Cloud Infrastructure, and (if a direct connection cannot be established), either by the worldwide network of stateless Jump Desktop Relay Servers, or by private, on premises Relay Servers, for enterprises that desire that Jump Desktop for Teams traffic does not traverse public networks

In all cases, Jump Desktop for Teams connections are encrypted end-to-end. None of the mediating entities is able to decrypt them.

All connections, whether successful or failed, are logged by Jump Desktop for Teams to facilitate forensic analysis. If a connection fails, an error message is displayed on the user's device.

How does Jump Desktop for Teams work?

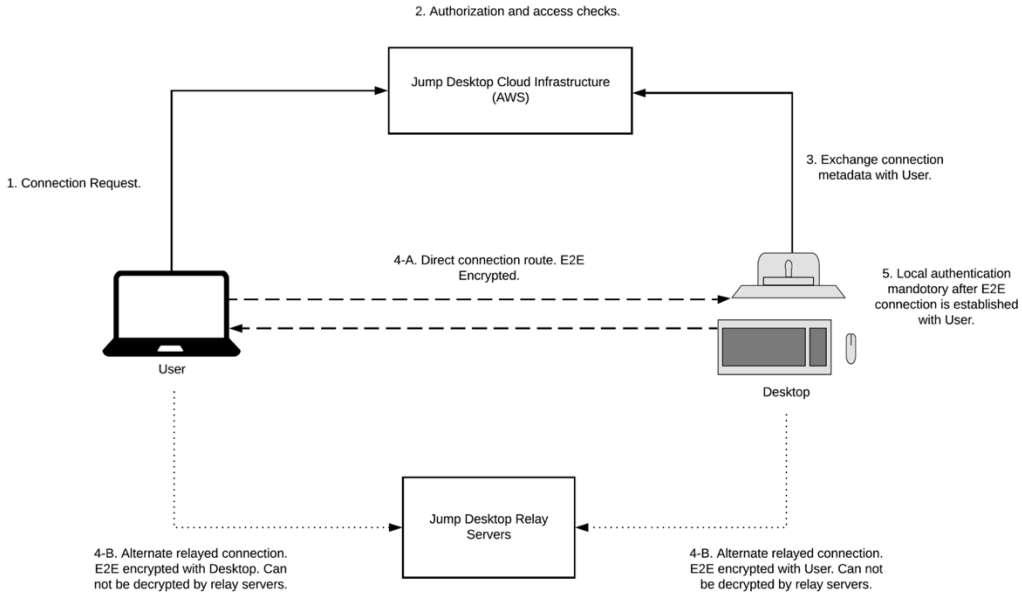
Initiating, Authenticating, and Authorizing the Connection

Is the connection allowed?

When a user initiates a connection to a remote computer, the AWS-based Jump Desktop Cloud Infrastructure authenticates the user and determines whether the user is authorized to access that particular computer. If the authentication or authorization fails, the connection is blocked, and an error message is displayed on the user's device.

Note: Jump Desktop ensures that all incoming connections authenticate locally before allowing access.

Jump Desktop Cloud Infrastructure



1. Jump Desktop Cloud Infrastructure

Establishing a Direct Connection

Can a direct connection be established?

If the authentication and authorization is successful, Jump Desktop attempts to open direct end-to-end encrypted connection between the user device and the remote computer.

If the attempt to open a direct connection between the user device and the remote computer fails (for example, if it is blocked by a firewall), Jump Desktop establishes a connection mediated by a Relay Server.

Connection Mediated by a Relay Server

If not, use a Relay Server

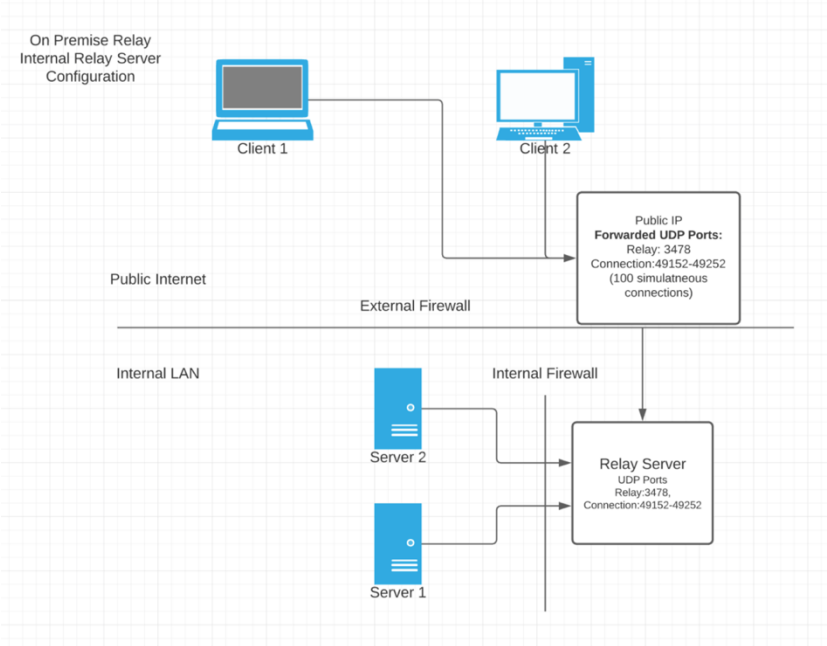
Depending on how Jump Desktop for Teams is configured, it will mediate the connection either by the worldwide network of stateless Jump Desktop Relay Servers or by the enterprise's private on-premises Relay Servers.

Note: Relay Servers, whether Jump Desktop or Private, cannot read Jump Desktop traffic, since it is encrypted end-to-end between the user device and the remote computer.

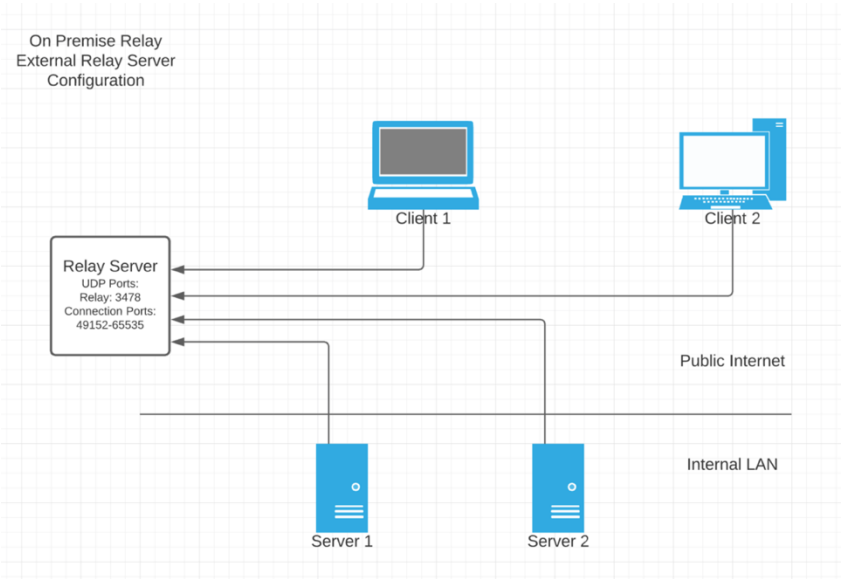
Jump Desktop Relay Servers
Jump maintains a worldwide network of Relay Servers that enterprises can use to mediate connections.

Private Relay Servers

Some enterprises may prefer, for security considerations or in order to minimize latency, to maintain their own private on-premises Relay Servers, either within their own networks (Figure 2) or in an adjacent DMZ (Figure 3).



2. Internally Hosted Private Relay Server



3. Externally Hosted (in DMZ) Private Relay Server

Mandatory Authentication After a Connection Has Been Established

Once the end-to-end encrypted connection has been established, whether directly or through a Relay Server, Jump Desktop implements yet another layer of security. Jump Desktop Connect running on the remote computer requires the user to authenticate with an account on the remote computer. Users can also authenticate with Microsoft Active Directory accounts or LDAP, if the machine is joined to a domain controller or directory services. This authentication step *cannot* be disabled.

Jump Desktop Connect does not allow accounts with empty passwords to connect remotely.

This authentication step happens directly over the end-to-end encrypted connection and is independent of the Jump Desktop Cloud Infrastructure.

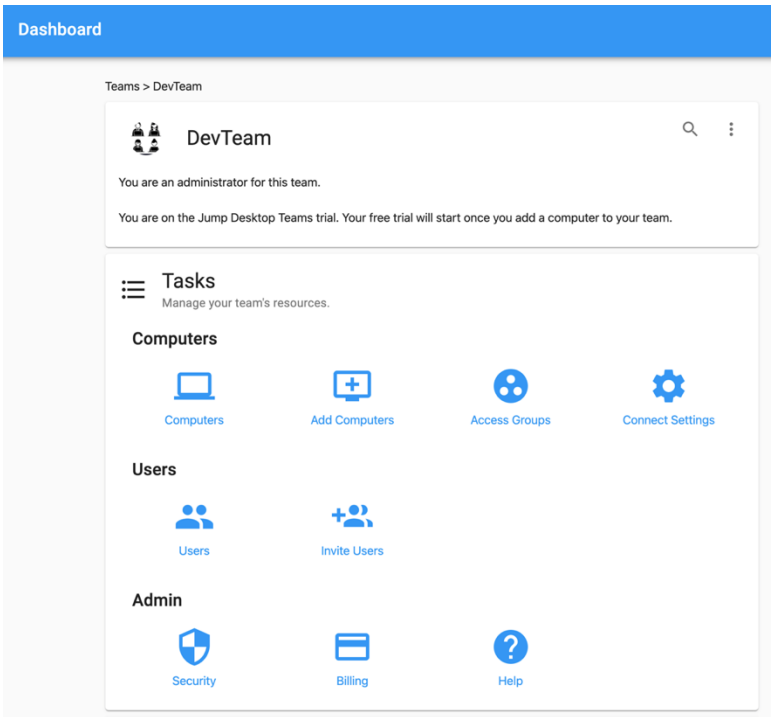
Logs

All connections, whether successful or failed, are logged by Jump Desktop for Teams to facilitate forensic analysis. If a connection fails, an error message is displayed on the user's device.

Centralized Access Control Management

Jump Desktop administrators have full access control for their team members. They can:

- grant or revoke users access to specific computers or to groups of computers,
- define access groups of users,
- define the computers that can be accessed by the team,
- define connection settings,
- enable Single Sign-On (SAML 2.0), two factor authentication (TOTP), or authentication via Google or Apple accounts,
- configure automatic disconnect after a defined period of inactivity,
- view details of active connections,
- enforce MFA if required.



4. Jump Desktop for Teams Access Control

Authentication and Authorization

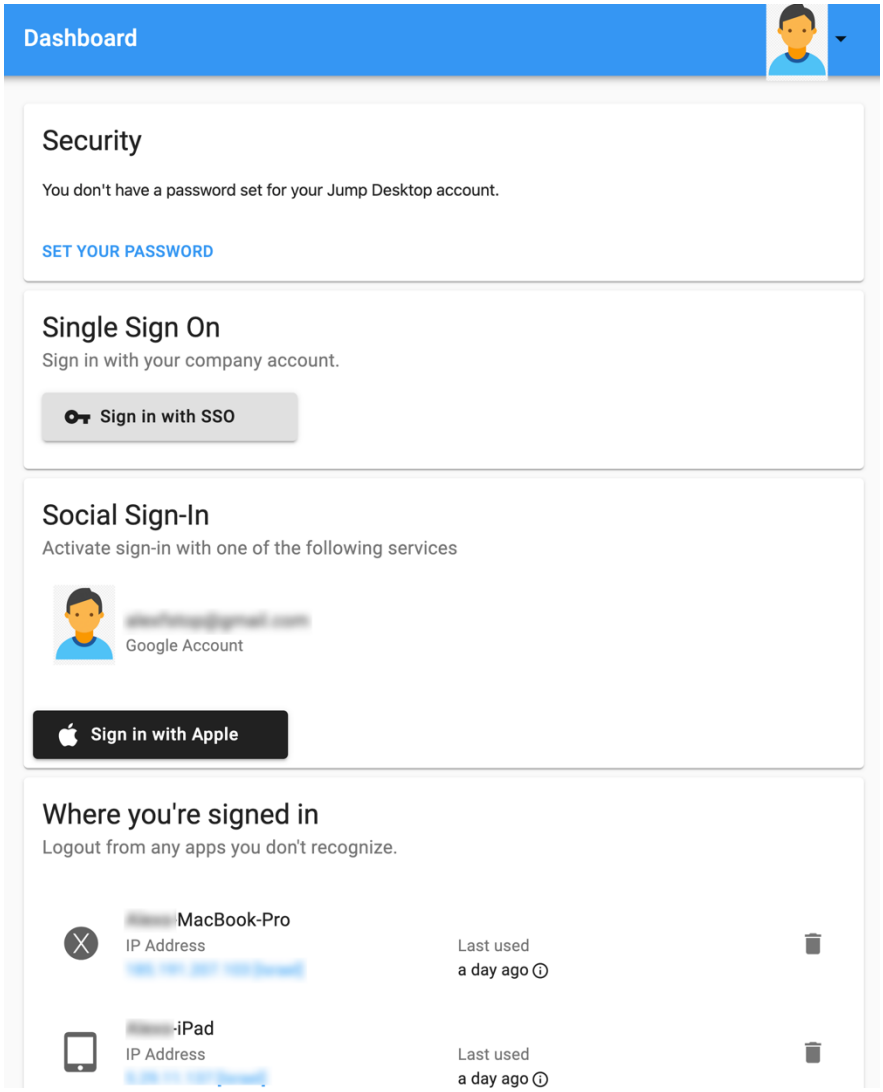
IT administrators can have confidence that their enterprise assets are not exposed to risks from unauthorized malicious actors because access is controlled by a two-stage process:

- Jump Desktop confirms that remote users are authorized to access the computers to which they are attempting to connect, based on permissions defined in Jump Desktop.
- Once users gain access to enterprise computers, their access to other enterprise assets (files, databases, processes, *etc*.) is controlled by the same access controls implemented for local users (Microsoft Active Directory, LDAP, *etc*.).

Users

Users can define their own passwords. The following additional authentication options are available to users, but the administrator must first enable them (Figure 5):

- Single Sign-On via SAML 2.0
- Enforcement of two-factor authentication
- Google or Apple accounts



5. Jump Desktop for Teams User Security

Special Features

VPN-Only Connections

Jump Desktop Connect (the client software that manages the Jump Desktop connection) can be configured to allow connections only when there is a direct networking path between the devices.

In this mode, Jump will not use Relay Servers or take indirect networking routes. For example, if a user tries to connect from a network where VPN is not enabled, the connection attempt will fail because Jump cannot find a direct route between the user and the target machine.

Note: In this mode, administrators must ensure that their firewall rules allow the VPN IP address pool to communicate over UDP with the host machines. Otherwise, connections will fail.

Cloudless Fluid

Jump Desktop's Cloudless Fluid feature enables even organizations whose networks are not connected to the internet (because of unique security requirements) to use Jump Desktop for Teams. Users connect using IP addresses, and the enterprise enforces authentication and authorization directly.

Jump Desktop API

Some Jump Desktop functionality (for example, adding computers to a team) can be implemented by other apps using the Jump Desktop API. The API provides access to all the functionality of the dashboard so that enterprise administrators can automate tasks.