Lenovo Unified Workspace

Security Overview

One of the surest ways to keep a company's datacenter safe? Eliminate remote access. Each time an employee initiates an outside connection, a string of security risks ensues—whether it's another click of the "remind me later" button for critical updates or an attempt to upload an infected file. This is a constant issue for IT, which in reality must continue to safeguard company resources as growing numbers of employees want, and even expect, the freedom to work from anywhere and on any device. Eliminating all threats to internal network resources during these remote connections is virtually impossible.

That is, unless you keep users at bay. And that's a job for Unified Workspace's two-tiered security architecture.

Unlike VPNs and hosted desktops, our two-tier setup ensures users never physically "touch" internal network resources. When security is fortified with a server-relay setup, employees can access all the apps and data they need without ever physically connecting to the network.

In this white paper, we'll provide a detailed overview of the Lenovo Unified Workspace two-tiered model and show how relay encryption, authentication, access control and server sessions are leveraged to provide a positive employee experience while safely keeping users an arm's length away from sensitive data.

TABLE OF CONTENTS

WORKSPACE SECURITY FOR ANYTIME, ANYWHERE ACCESS

Today's companies are moving fast to meet the needs of customers, partners and employees. They want to allow easy access to applications and data from varied locations and devices while maintaining security and control and accounting for that access. Lenovo Unified Workspace assists companies in meeting these very challenging objectives.

As 9 to 5 becomes 24/7 and employees rely less on company-owned, IT-managed PCs to get things done, they want the flexibility to work on any device—at any time and from anywhere.

Web-based technologies have made this possible, but there is a catch. Many of the most-used solutions are effective at securing sensitive data only after a user has initiated a connection. This has many companies asking:

- How do you provide the convenience of a web-based work environment…without becoming a victim of the web itself?
- How does a company maximize security when so many devices lack IT oversight?
- How can IT make apps and data readily available on a wide variety of devices and operating systems—without exposing internal resources?

Lenovo Unified Workspace leverages security protocols that go beyond those of other solutions such as Virtual Private Networks (VPNs) and hosted desktops. This workspace aggregator provides single sign-on access to all apps and data in an HTML5-based work area, *without ever connecting remote users directly to the company datacenter.*

The Unified Workspace architecture adds layers to your existing security, allowing authorized users a consistent web-based work experience. All they need is an HTML5-aware browser and permission to safely access resources.

EXTEND EXISTING IT INFRASTRUCTURE

Chances are, you have all the key components necessary to support BYOD policies and distributed workforces: public cloud services, private apps and a VPN for remote access. Unified Workspace has been engineered to embrace all of your existing solutions and unify them in a more secure, single sign-on (SSO) web-based environment. The solution has been architected to embrace many existing security measures, from content filters to directory services.

THE FOUNDATION: TWO-TIER ARCHITECTURE

Unlike VPNs, Unified Workspace keeps users physically separated from internal assets.

Connecting Users to Company Resources

The foundation of Unified Workspace is a server-based, two-tier architecture that physically separates end users from internal network resources. Employees may *think* they're connecting directly to company data—the user experience is the same across devices—but are in fact kept at arm's length from the datacenter.

Here's how it works:

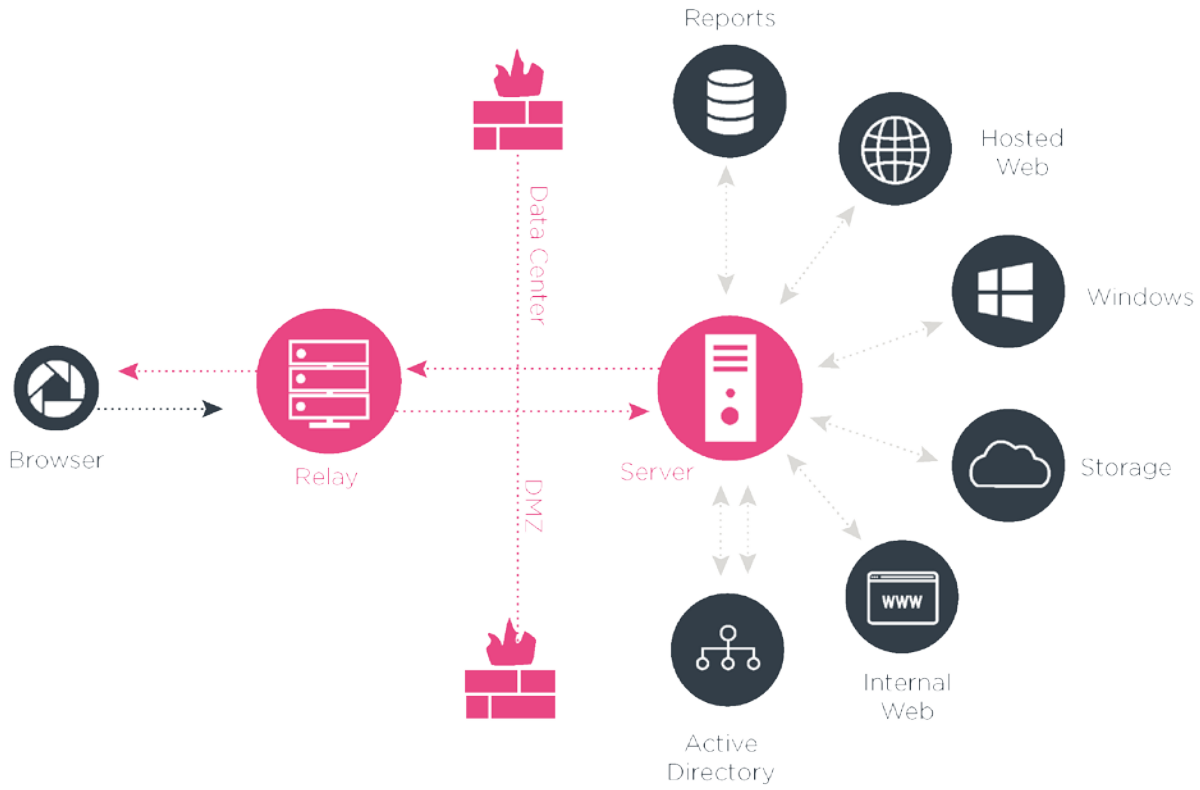
The Unified Workspace architecture consists of two main components:

1. The Server

A dedicated Unified Workspace server sits on-premises, inside the company's datacenter, and acts as the secure entry point. This server is responsible for authentication, access control, service execution, clustering and directory services communication. The server is designed to communicate with both the network directory service and internal IT applications and services.

2. The Relay

A Unified Workspace relay sits in the company's demilitarized zone (DMZ). The relay's primary function is encrypting all traffic between devices and the Unified Workspace private cloud through Secure Sockets Layer (SSL). It's designed to create a secure connection between the user and internal resources and render the web-based workspace safe. A Web Application Firewall (WAF) sits in front and behind the company's demilitarized zone. The WAF has Intrusion detection (IDs) and Intrusion Prevention (IPs) systems, these two systems will detect and prevent any malicious traffic that comes into UWC. The process is automated and will block in appropriate requests. The IPs and IDs will monitor any changes in the application for auditing and monitoring.



While the footprint of these two foundational components is minimal, the layers of security they add are significant.

Private IT applications in the datacenter can be accessed by remote users and are given controlled access from the DMZ through a single, secure port. This ensures your data and applications are secure and available when needed. Security is further enhanced by funneling traffic through a single encrypted address, making firewalls and rules much less complex.

THE LAYERS: AUTHENTICATION, ENCRYPTION AND ACCESS CONTROL

The server and relay work together to implement security features at multiple levels.

The Unified Workspace server is placed inside the customer network so it can access internal resources, and is responsible for:

SSL relay encryption

As users are isolated in the DMZ and prevented from physical access to the network, the relay encrypts all communications between the end user and the Unified Workspace private cloud in SSL. All requests made from the browser for internal resources are made by the relay, and any application or service retrieved from the private cloud is encrypted before being communicated over the public web.

Pipeline services

A user's request for an application is redirected by the Unified Workspace relay to the Unified Workspace server inside the data center. The Unified Workspace server then communicates directly with the application server to fulfill the request.

Authentication

Unified Workspace embraces your existing directory service for users and group membership as well as authentication. Supported directory services include:

- Microsoft Active Directory
- Novell eDirectory
- OpenLDAP
- OpenDJ

The Unified Workspace server authenticates users by taking the credentials they enter and validating them against the network directory service. Initial login is secured by a variety of two-factor authentication (2FA) methods including:

- Image challenge
- CAPTCHA
- RADIUS tokens
- One Time Passwords (OTP)

Once authenticated, employees are granted SSO access through a single user ID and password that can be used on any device without compromising the network. Unified Workspace can leverage the following industry standard authentication protocols to provide users with seamless authentication into the applications they use every day:

- SAML 1.1
- SAML 2.0
- NTLM
- ADFS
- Shibboleth

For other applications that are not configured to interact with the directory or leverage a standard like SAML, Unified Workspace offers a form-based authentication system called webPass. The first time a user wants to access one of these apps, he or she is prompted to enter an existing username and password. The information is encrypted using the AES-256 symmetric key cipher and is stored centrally as an attribute in the attached directory service.

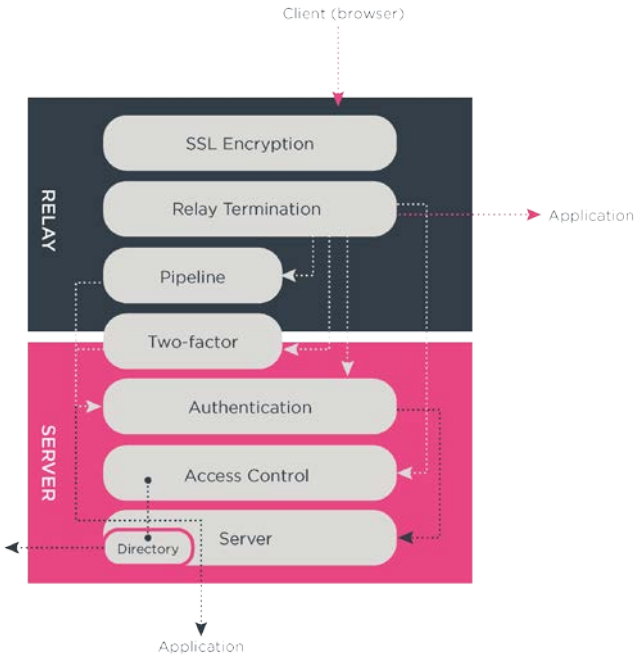
Role-based access

As remote users are given controlled access from the DMZ, private IT applications stay safe in the datacenter. The level of access each employee has to company file systems, internal and hosted web and SaaS applications, and even remote desktops is determined by the access control list. This Access Control List (ACL) is determined by IT and dictates which specific resources an authenticated user will be able to access when connecting remotely.

While the relay does not decide which data users can access, it does enforce ACL decisions dictated by the Unified Workspace server. When the server denies access to a service, the relay will enforce the server's decision and deny the user access to the requested resource or application.

Server Sessions

Once a user has been authenticated to the system, the server configures a session especially for the individual. The relay is responsible for rendering this personalized workspace interface, which is dynamically created based on the employee's profile, access control list, personal settings and device type.



The server and relay work together to implement layers of security throughout the product, with each Unified Workspace instance performing a very unique and specialized function.

Optional Secure Browser

For any app or data an organization deems to be especially sensitive, there's the option to use Quarri Data Safe™. This web security solution has been integrated into the Unified Workspace ecosystem to further secure content at the device level. It protects browser-delivered information on unmanaged endpoints to defend against malware and user-driven leaks—all while allowing users to remain productive in a seamless, browser-based Unified Workspace experience. Any time you determine an application or site requires a higher level of security, IT

can configure the session so that a user will be directed away from default browsers and into the Data Safe browser. This configuration provides:

- Malware defense by scanning processes during a user session to identify and block key logging and screen capture applications
- Encryption of all disk-based session data such as cookies, cache, history and temporary files
- Restriction of endpoint information leakage through means such as copying and pasting, file saving, printing and screen capturing
- Blockage of hostile code injection attacks and vulnerable browser add-ons, as well as defense against zero-day attacks

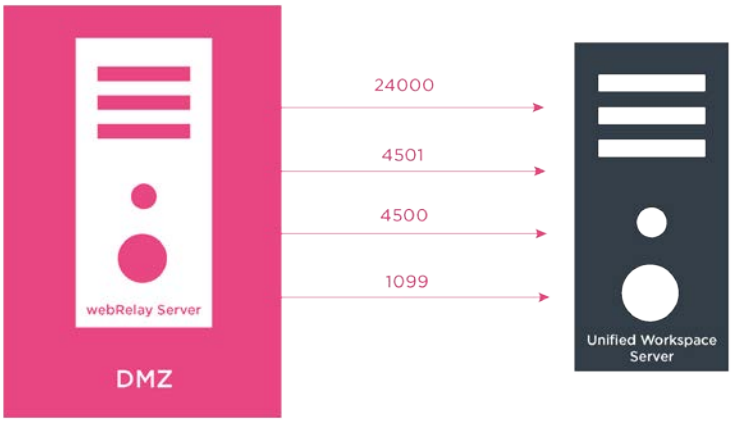
THE COMMUNICATIONS: HOW TRAFFIC FLOWS

Because Unified Workspace is built on a two-tier architecture and integrated between the data center and DMZ, it's important to understand how the system components communicate.

Relay to Server

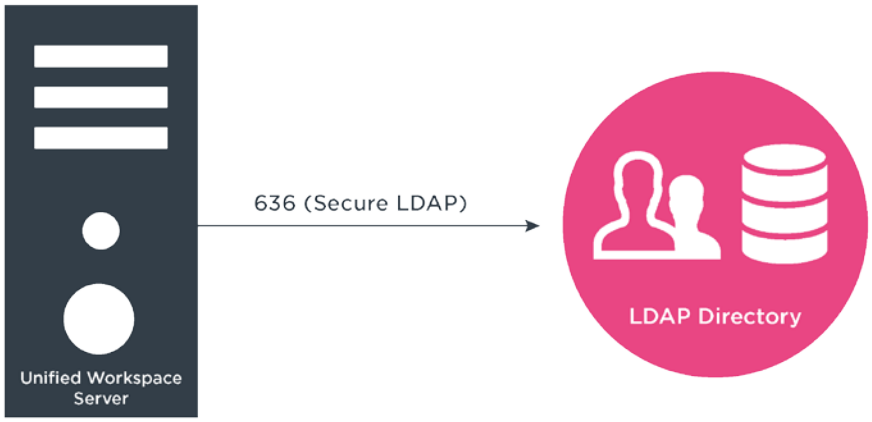
Most often, the relay is located on-premises within the organization's DMZ and the server is deployed within the data center. The firewall between the two devices is then configured to allow communications via the four default ports used between server and relay.

- Registry Port (default 1099) and Service Port (default 4500): These are the ports on which the server will listen for relay discovery requests.
- Optional Pipeline Port (default 4501): A single port is used between the server and relay for communicating with internal data center applications, servers and services.
- Optional Relay Central (default 24000): This communication port is used by the relay to get content updates—for style, HTML, CSS, images and so on—from the server.



Server to Directory

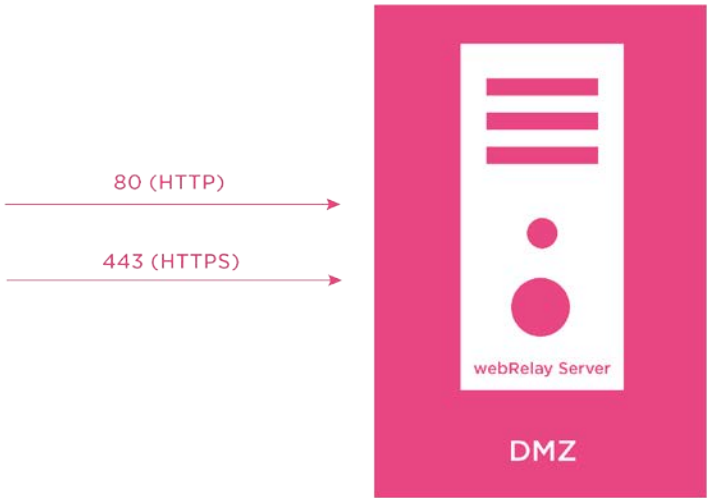
By default, the Unified Workspace server communicates with the internal directory service via Secure LDAP over port 636.



User to Relay

Communication between the end user and Unified Workspace are enclosed within the SSL protocol, which simplifies the configuration of any device that might sit in front of the Unified Workspace relay. To perform its job as system entry point, the relay uses:

- HTTPS (SSL) (Default Port 443): This is the port on which the relay will communicate with the end user's browser as all traffic is encrypted.
- Optional HTTP (Default Port 80): The port on which the relay will redirect any request automatically back to secure port 443.

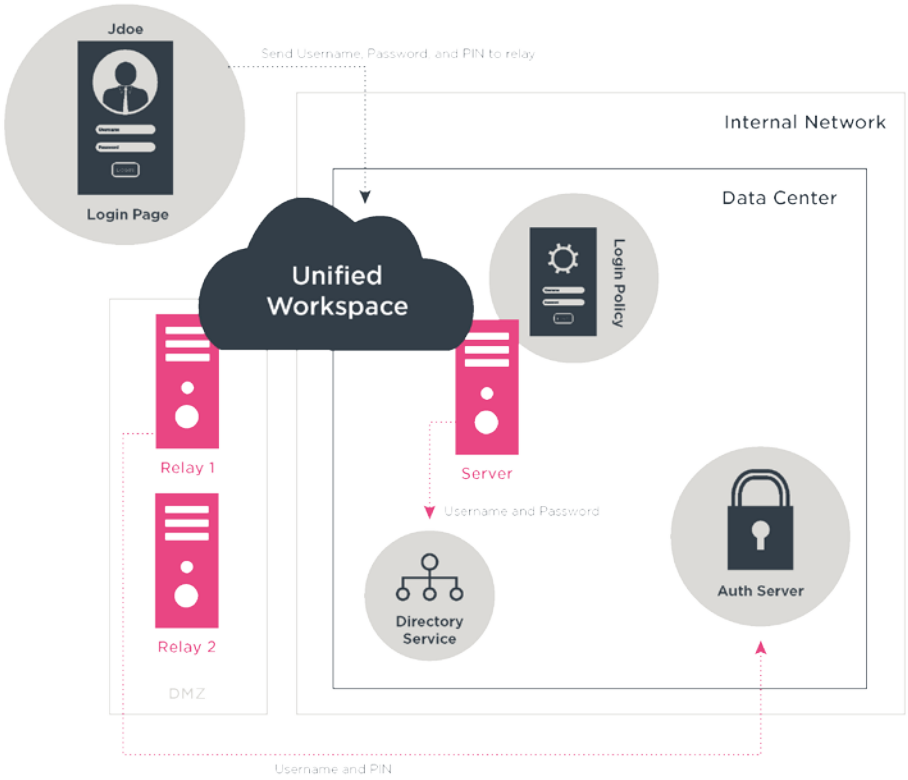


Authentication Methods

Unified Workspace supports a variety of authentication methods. By default, network usernames and passwords will always be used to authenticate users. The system supports many other methods for two-factor authentication including Image Challenge, CAPTCHA, challenge questions, RADIUS tokens, One-Time Passwords (OTP), and acceptable use policies.

Token Authentication is widely used with Unified Workspace. Enabling RADIUS authentication modifies the login process to require PIN numbers in addition to usernames and passwords. This PIN number is typically generated by a token that works in conjunction with a backend authentication server via RADIUS or by using a time-based one-time password generator.

During token authentication, the Unified Workspace relay passes the username and PIN to the backend authentication server (via RADIUS) for validation. At the same time, the username and password is also passed to the Unified Workspace server. If both sets of security credentials are accepted, the user proceeds with the login process to access his or her workspace.



The specific authentication methods used are determined at the administrator level based on organization-specific requirements and security needs. Once that's determined, the server and relay will work together to manage the authentication process. As the relay builds a user login page, the server reads the login policy to determine requirements for authentication. The login page then changes to meet them.

Meanwhile, employees see a digital interface that's consistent across different devices and provides easy access to all the apps and data they need to be productive.

Additional Resources

For browser requirements, supported databases and specifications, visit:
http://www.lenovosoftware.com/support/unified-workspace/specifications

---

Lenovo Unified Workspace empowers IT to deliver more flexible, agile and collaborative workplaces and meet evolving employee expectations. This workspace aggregator both modernizes and simplifies IT management with anytime, anywhere, any device access to public or private web-based apps, legacy Windows apps, remote desktops and file shares.

Lenovo is a $46 billion global *Fortune 500* company and a leader in providing innovative consumer, commercial and enterprise technology. Our portfolio of high-quality, secure products and services covers PCs (including the legendary Think and multi-mode YOGA brands), workstations, servers, storage, smart TVs and a family of mobile products like smartphones (including the Moto brand), tablets and apps.

Learn more at lenovosoftware.com/unified-workspace.