Remote Access for Industrial Control Systems

DISPEL.io

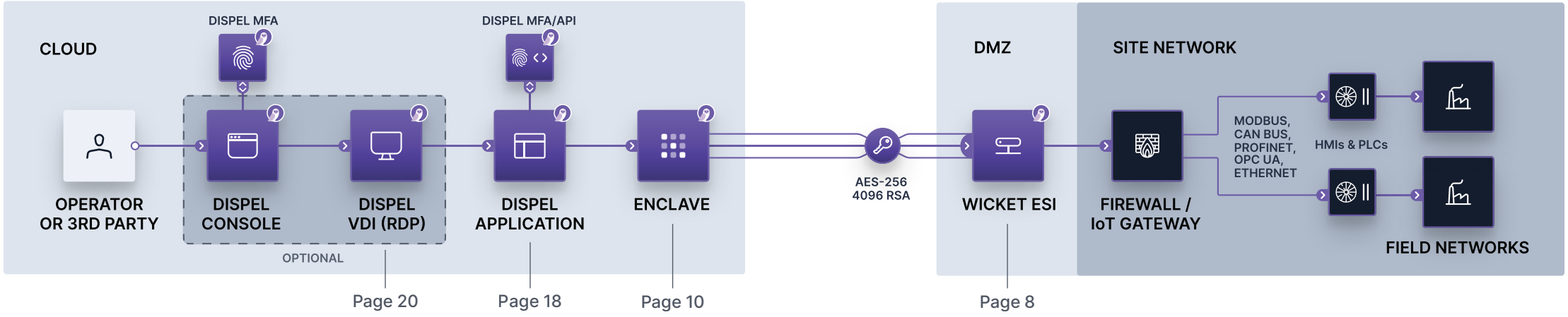

CLOUD
DISPEL MFA
DISPEL MFA/API
OPERATOR
OR 3RD PARTY
DISPEL
CONSOLE
DISPEL
VDI (RDP)
DISPEL
APPLICATION
ENCLAVE
OPTIONAL
AES-256
4096 RSA
DMZ
WICKET ESI
SITE NETWORK
FIREWALL /
IoT GATEWAY
MODBUS,
CAN BUS,
PROFINET,
OPC UA,
ETHERNET
HMIs & PLCs
FIELD NETWORKS
Page 20
Page 18
Page 10
Page 8

Table of Contents

What Is This?

The purpose of this manual is twofold: (1) To provide deep technical understanding of the various components of Dispel's remote access platform, and (2) to aid during the implementation planning phase so that our customers understand fully the Networking Requirements, Cloud Implications, and Connection Processes imposed by our system.

– Dispel

Components

Wicket ESI

What is a Wicket ESI?

Wicket ESIs are on-premise components that let your team connect to ICS remotely without having to install software onto pre-existing ICS equipment.

Is it hardware or software?

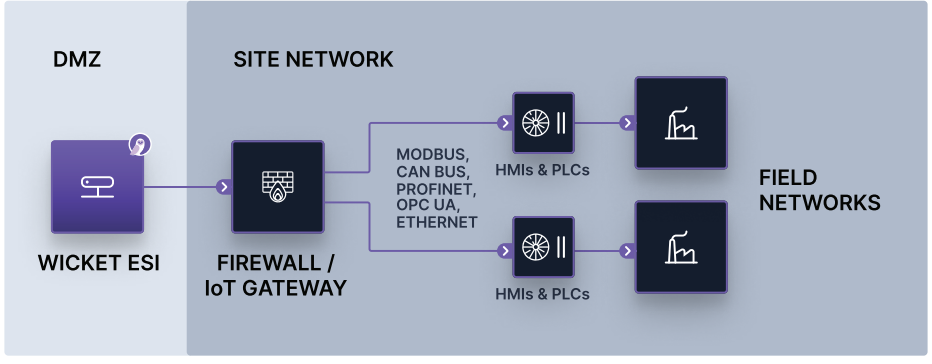
Wicket ESIs come as either hardware or, if you would prefer to use your own servers, a virtual appliance. The underlying OS is Ubuntu.

What does it do?

(1) Establish an encrypted connection to an Enclave (Page 10).
(2) Enable connections to ICS devices as permitted by an internal whitelist.

Is it automated?

Yes. A Wicket ESI will proactively reach out to (re)establish an encrypted connection to an Enclave. Wicket ESIs can be arrayed to provide multiple tiers of hot redundancy.



FIREWALL RULES

```
OUTBOUND 1194  [ENCRYPTED TUNNEL TO ENCLAVE]
OUTBOUND 443   [HTTPS - FOR CREDENTIAL MANAGEMENT]
OUTBOUND 22    [SSH - INSTALLATION/REMOTE SUPPORT]
```

Enclave

What is an Enclave?

An Enclave is a group of Virtual Machines (VMs) leased from Public or Private Clouds and networked together over private interfaces [10.8.X.X]. Enclaves are Moving Target Defense networks.

How long do they take to build?

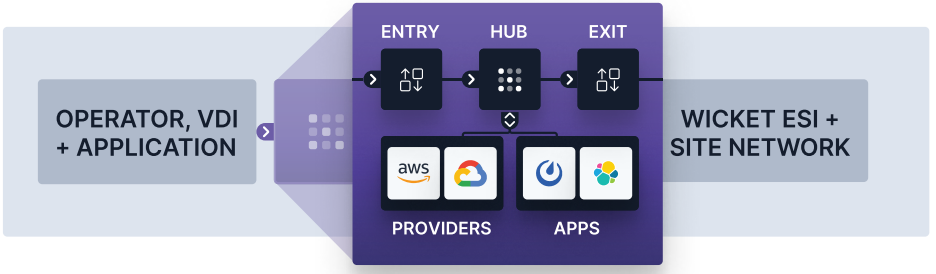
15-30 minutes.

What does it do?

An Enclave provides a non-attributable pathway for end-to-end encrypted connectivity to either a Wicket ESI or cloud resources into the Enclave.

Technical Specifics

Enclave components are primarily deployed atop an Ubuntu 16.04 LTS OS. For some of our Virtual Desktops, we deploy a Windows 2016 Server. The size of each VM varies by function.



VM OS	UBUNTU 16.04 LTS | WINDOWS 2016
VM SIZES	2-4 vCPU | 4-16 GB RAM | 50 GB STORAGE
ENCRYPTION	2X AES-256 WITH 4096-BIT RSA
CLOUD PROVIDERS	AWS, AZURE, GOOGLE CLOUD, DIGITALOCEAN, VMWARE SOFTLAYER, RACKSPACE, VULTR, CLOUD SIGMA, OPENSTACK

Dispel Engine

What is the Dispel Engine?

A Dispel Engine builds Enclaves, Virtual Desktops, and other virtual components. Engines have three components: (1) the Build API; (2) the Console; and, (3) the Identity Controller.

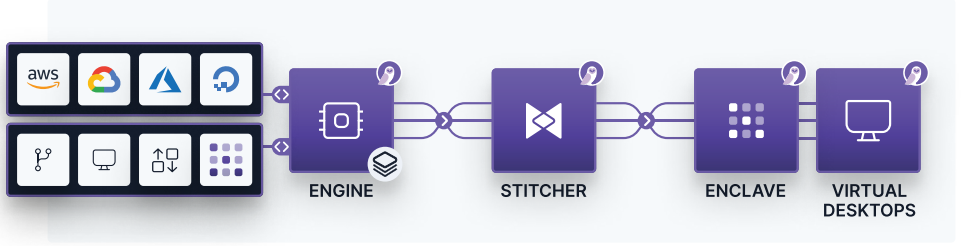
Where does it sit?

Dispel can deploy an Engine either as a hardware device on your property, or as a virtual appliance on hosted on Public or Private clouds.

Build API: leases VMs from cloud providers, applies build scripts/updates, and oversees network construction and maintenance.

Console: an web interface for managing the system and controlling user access.

Identity Controller: the validator of user credentials. Frequently integrated with LDAP or Active Directory.



FIREWALL RULES	BI-DIRECTIONAL	443	[CLOUD APIS & USERS]
	OUTBOUND	22	[APPLY BUILD SCRIPTS TO VMS]
	INBOUND	22	[INTRA-ENGINE COMMUNICATION]

Engine – Cloud Deployment

Cloud Deployment

An Engine can be deployed on either Dispel's or the Customer's cloud accounts. If the latter, an Engine License is needed.

Virtual Machine Specs

The specifications will vary based upon concurrent VM build requirements. For standard deployments, we recommend 8 vCPUs, 32 GB RAM, and 500+ GB SSD Disk.

Benefits Cloud Deployment	
Same day deployment	✓
Optional single tenancy	✓
Control of encryption keys	✓
More robust SLA options	✓
Swift disaster recovery	✓
Deploy in 150 global datacenters	✓

Engine – On-Prem Deployment

On-Premises Deployment

The Dispel Engine may also be deployed on-premises. This option generally makes sense for customers with on-prem resources who currently do not wish to move to the Cloud.

Hardware/VM Specs

For standard deployments, we recommend a multi-server (3 servers) layout, each with 4 vCPUs, 16 GB RAM, and 250+ GB of SSD disk space.

Benefits On-Prem Deployment	
Single tenancy	✓
Encryption keys on-prem	✓
Swift disaster recovery	✓
Regulatory considerations	✓
Total integration into existing security framework	✓

Engine – Hybrid Deployment

Hybrid Breakdown

The Console must be able to receive all HTTPS traffic in order for users to access it. If you want the smallest possible attack surface, we recommend placing the Build API and Identity Controller on your premises, and positioning the Console in a public cloud.

This layout means the on-prem Engine components need only receive a single connection.

Benefits Hybrid Deployment	
Single tenancy	✓
Encryption keys on-prem	✓
Collocation of firewall rules	✓
Regulatory considerations	✓
More robust SLA options	✓

Application

What is the Dispel Application?

The Dispel Application is a cross-platform client that creates an end-to-end encrypted connection from the host device up to a deployed Enclave.

How long does it take to connect?

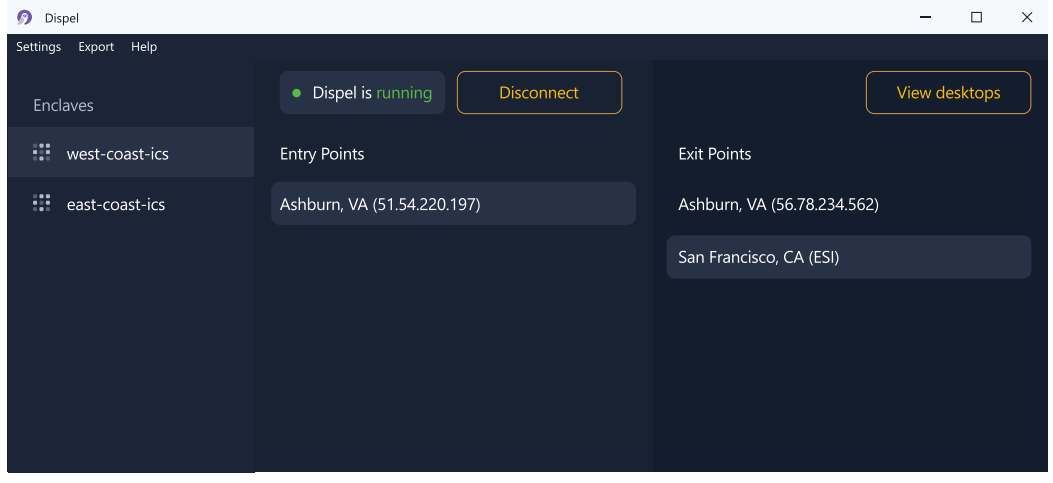
Connecting to, and switching between, Enclaves generally takes under 9 seconds if the Entry Points are located in the same country as the User. Switching between an Exit Points generally takes less than 5 seconds.

More on Encryption

All connections to an Enclave are protected within 2x layers of AES-256 with independent 4096-bit RSA for initial key exchange.

Endpoint Lockdown

The Dispel Application, when connected, ensures all traffic leaving the device passes through an Enclave. If you don't want your Users browsing the web while accessing an Enclave, they won't be able to.



Scan to see a video of our application and how it works.
https://dispel.io/remote-access-application

Virtual Desktop

Virtual Desktop Overview

Virtual Desktops serve as portals through which a user can reach an asset from an untrusted computer without passing malware from their device to the asset.

Relentless Patching

You want your systems kept up-to-date. Dispel's virtual desktops build with the latest patches every time.

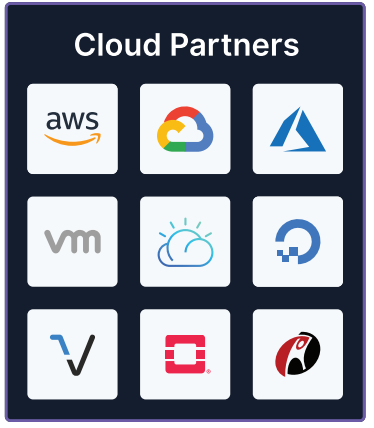
Unparalleled Customization

The Dispel Team will work with you to create a list of allowed applications and functions - including vendor specific applications, drive forwarding, and session recording.

Intuitive Inventory Management

You can control precisely how many virtual desktops are available every hour to be drawn upon by your team.

Dispel Virtual Desktops Features and Specs	
On-Demand Scalability	✓
Automated Patching	✓
Full Desktop Functionality	✓
Customized Applications	✓
Recording/Auditablility	✓



Scan to see a video of our virtual desktops in action.
https://dispel.io/remote-access-application

Session Recording

Session Recording

You can see exactly what your users are doing, and have done, on your virtual desktops.

Storage Options

You can keep recordings on a cloud server inside of an Enclave, or pull them inside your perimeter for long-term storage.

Storage needed for recordings
(Users) x (Days) x (~2.4GB)

	30 days	60 days	120 days
10 users	**720GB**	**1.44TB**	**2.88TB**
50 users	**3.6TB**	**7.2TB**	**14.4TB**
100 users	**7.2TB**	**14.4TB**	**28.8TB**
200 users	**14.4TB**	**28.8TB**	**57.6TB**

Session Recording and Live View
Features and Specs

Capture All VDI User Actions	✓	Require Recording to Connect	✓
Efficient RDP-only Storage	✓	Variable Speed Playback	✓
Configurable Retention	✓	Watch Live	✓
“Save Forever” Functionality	✓	Quickly Identify Idle Time	✓
Redundancy Options	✓	Simple Admin Dashboard	✓

Scan to see a video of our session recording functionality.
https://dispel.io/remote-access-recording

How everything connects

1 Enclave Created by Engine

1.1: Admin Launches Enclave

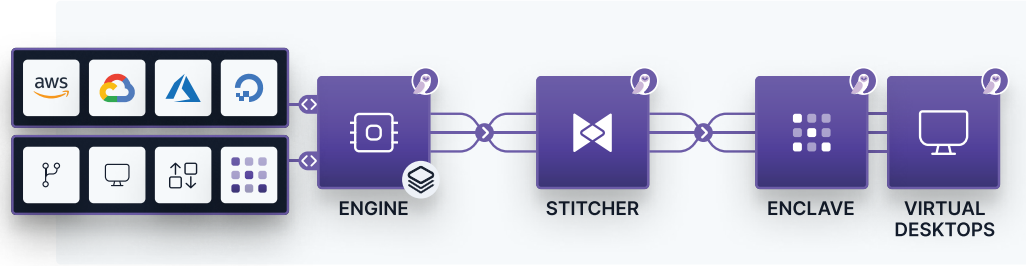
An Administrator determines the geographic location and constituent components of an Enclave. This request is sent to the Build API which invokes a sub-component, **Stitcher**, to apply build scripts and stitch the Enclave's internal network together.

Components:

[Traffic]	Hub	Entry	Exit
[Desktop]	Linux	Windows	Logging

1.2: Admin Adds Users

The Admin adds the appropriate users to the Enclave. If integrated with a customer's Active Directory, users will auto-populate the invite-field. Non-Active Directory user invitations are requested via email.



2 Wicket ESI Connects to Enclave

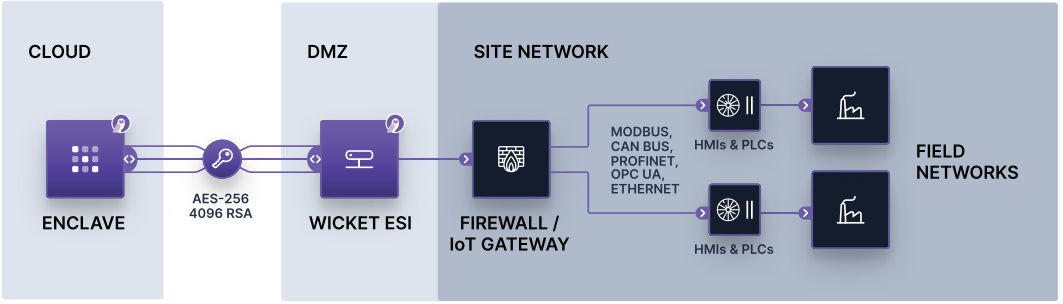
2.1: Wicket ESI Authenticates

The Wicket reaches out to a specialized applet, called **Fragment**, which contains the connection information for the Enclave it has been assigned to. Each Fragment is periodically updated (push only) by the Identity Controller.

Once the Wicket ESI receives the connection information, it reaches out to authenticate with the Enclave.

2.2: Wicket Establishes Connection

The Wicket ESI establishes an end-to-end encrypted tunnel to the Enclave and registers itself as an Exit Point.



3a User Reaches ICS

For Trusted Users on Trusted Devices

3a.1: User Logs Into Application

The user logs into the Dispel Application and enters their credentials/MFA.

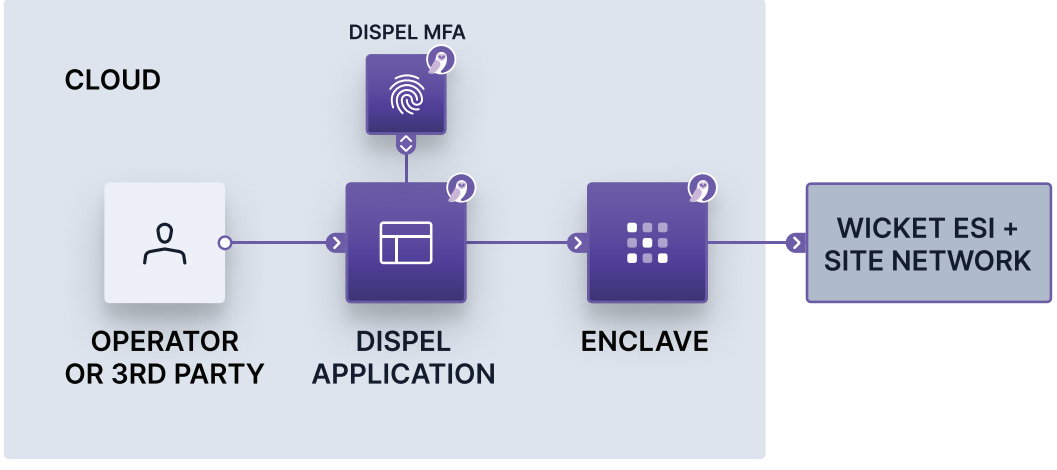
3a.2: User Connects to Wicket ESI

The user selects the Enclave and, then, Wicket ESI they want to reach.

3a.3: User Connects to ICS

Leveraging the tunnel to the ICS network, the user is now able to connect to the ICS devices that have been whitelisted by the Wicket ESI over the protocols allowed by the customer's firewall.

(The user chooses the appropriate Purdue Model Layers 3 & 4)



3b User Reaches ICS

For Semi-Trusted Users on Trusted Devices

3b.1: User Logs Onto Console

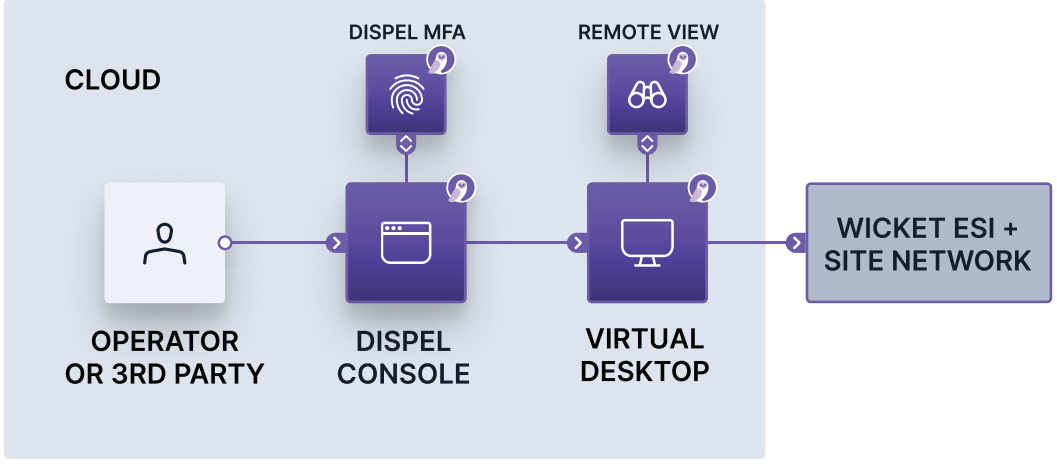
The User logs into the Dispel Console with their email, password, and multi-factor authentication token.

3b.2: User Selects Wicket ESI to Connect To

The User chooses the Wicket ESI they need to reach from a list showing only those to which they have been granted access.

3b.3: User Connects to ICS

The User is presented with a Virtual Desktop in-browser or, if Windows is desired, via RDP. The virtual desktop presents the User with the available ICS connected to the Wicket ESI. All of the User's actions are recorded and, if desired, live-streamed to an Admin.



3c User Reaches ICS

For Untrusted Devices

3c.1: User Logs Into Application

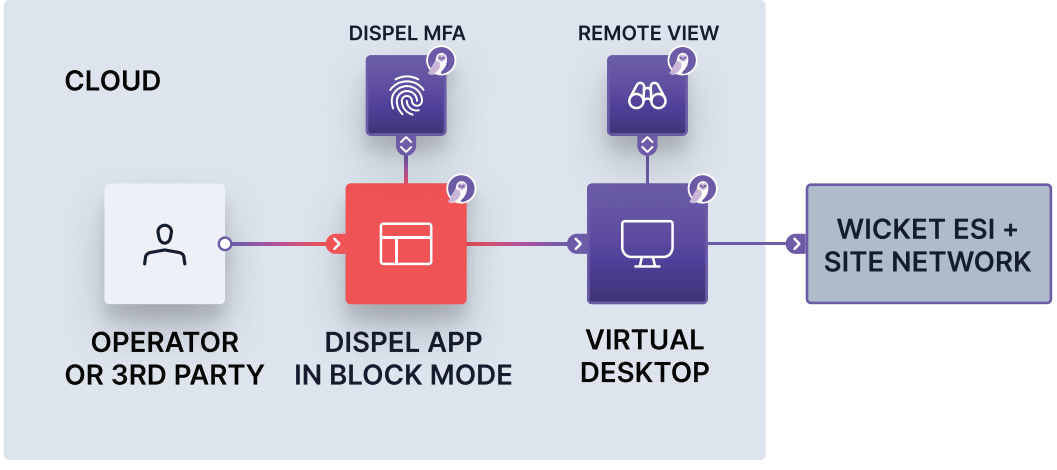
The user logs into the Dispel Application and enters their credentials/MFA. To prevent remote hackers from accessing the untrusted device while it is connected to the ICS, the application blocks all inbound traffic except from the connected Enclave.

3c.2: User Selects Wicket ESI to Connect To

The User chooses the Wicket ESI they need to reach from a list showing only those to which they have been granted access.

3c.3: User Connects to ICS

The User is presented with a Virtual Desktop in-browser or, if Windows is desired, via RDP. The virtual desktop presents the User with the available ICS connected to the Wicket ESI. All of the User's actions are recorded and, if desired, live-streamed to an Admin.



For the decision maker

Key Benefits

Dispel Remote ICS Access Platform Benefits and Value Adds			
Simple, Secure Login	✓	Session Recording	✓
Fast, Stable Installation	✓	Strong E2E Encryption	✓
Moving Target Defense	✓	Multi-Factor Authentication	✓
Network-Level Access Control	✓	Reduce/Remove O&M Costs	✓
Cloud Agnostic Capabilities	✓	Simple Admin/Scheduling	✓

Case Study

ConnecticutWater

Project Overview

Dispel was contracted by CT Water to implement a remote access solution to their ICS (SCADA) Environments.

What were the results?

Dispel currently provides remote access for CT Water Operators working on company HMIs & PLCs. Further, CT Water has replaced their traditional corporate VPN with Dispel, and provides vendor/3rd party access via Dispel Virtual Desktops.

CT Water - ICS Connectivity Key Metrics	
87% Faster Operator Login	✓
$980,000 Efficiency Savings	✓
10-15x Direct ROI	✓
Active Directory Integration	✓
Fully Redundant System	✓
Session Recording: 3rd Parties	✓

Competitive Analysis

Competitive Analysis How Dispel is Different	
Globally Deployable	✓
Moving Target Defense	✓
Integration Flexibility	✓
Faster Operator Login	✓
Post-Quantum Encryption	✓
Zero Site-Network Interference	✓

Globally Deployable

Dispel's Enclaves and Virtual Desktops can be deployed in over 150 global datacenters or on private clouds controlled by the cutomer.

Moving Target Defense

Enclaves and VDIs can be destroyed and rebuilt on a schedule or on-demand, creating an ever shifting model that frustrates attackers trying to gain a foothold. You now hold the benefit of time, not attackers.

Integration Flexibility

Dispel's system can quickly integrate with your Active Directory, PAM systems, Data Diodes, or other security measures you have in place.

Faster Operator Login

Operators and 3rd parties love the simplicity of Dispel's login. They are accustomed to a VPN style login, with their phone for MFA. We give that to them — providing security without sacrificing simplicity or speed.

Post-Quantum Encryption

All connections to-and-within an Enclave are encrypted with two layers of AES-256 with 4096-bit RSA for initial key exchange.

Zero Site-Network Interference

By positioning the Wicket ESI external to the Site-Network, Dispel's remote access solution operates without creating any down-time risk.

enterprise@dispel.io | dispel.io