

CACHATTO®

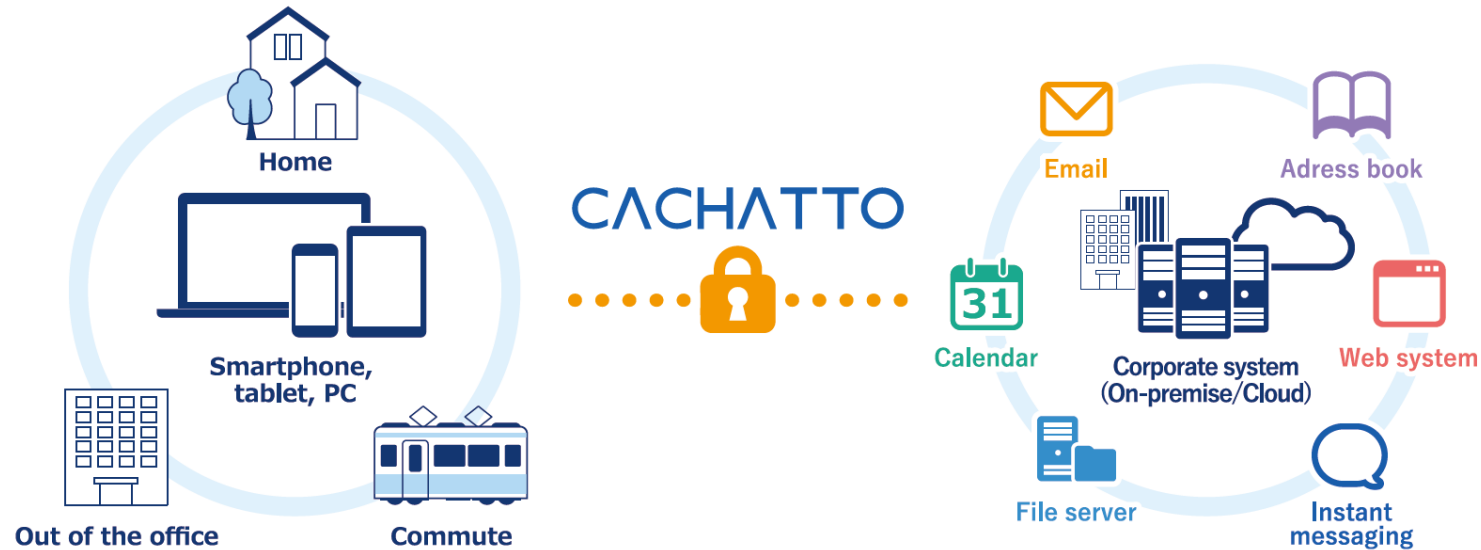
Remote access solution

What is CACHATTO?

Provides a secure resource access environment

CACHATTO is a remote access service that enables users to conveniently access to the intra/cloud business system in a single secure platform from a variety of devices.

It ensures a delivery of the right applications and resources to the right users, at any time and in any location without the need for VPN nor firewall settings changes.



What is CACHATTO?

Simple to deploy data access solution

- Secure access and Data Leak prevention
 - No enterprise data stored on mobile device
 - Corporate and personal data/applications completely isolated on end devices; no cross-contamination
 - End devices do not have direct access to the corporate network/servers
 - Prevents security breaches through Multi-factor authentication (MFA) and built with SSO capability
- Consistent and comprehensive
 - Device agnostic
 - Supports wide range of devices and OS versions
- Robust architecture
 - Identity-centric network connection - Individualized access parameter
- Ease of installation and deployment
 - No VPN nor changes in the firewall settings necessary
 - Easy user and resource management
 - Simple installation and setup of the CACHATTO application on client devices

What is CACHATTO?

Security and Data leak prevention

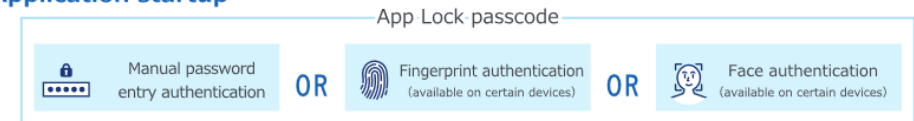
CACHATTO prevents security breaches by not having direct access to the corporate network.
Preventing any data leakages by restricting storing of data on client device

Multi-factor authentication

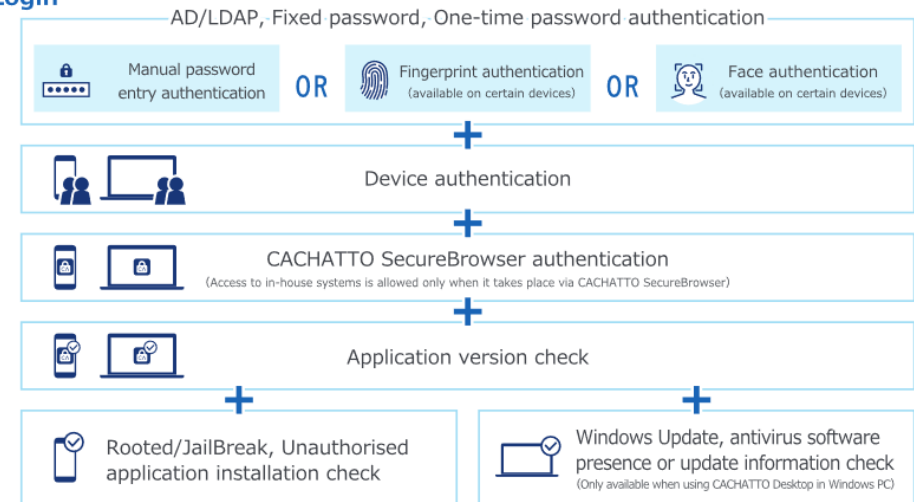
Multi-factor authentication guarantees a high level of security by utilizing authorisation process when logging in:

- App Lock
- AD/LDAP login
- Device authentication
- SecureBrowser authentication
- Application version check
- Rooted/Jailbreak check
- Unauthorised application installation check

Application startup



Login



What is CACHATTO?

Individualized access perimeter

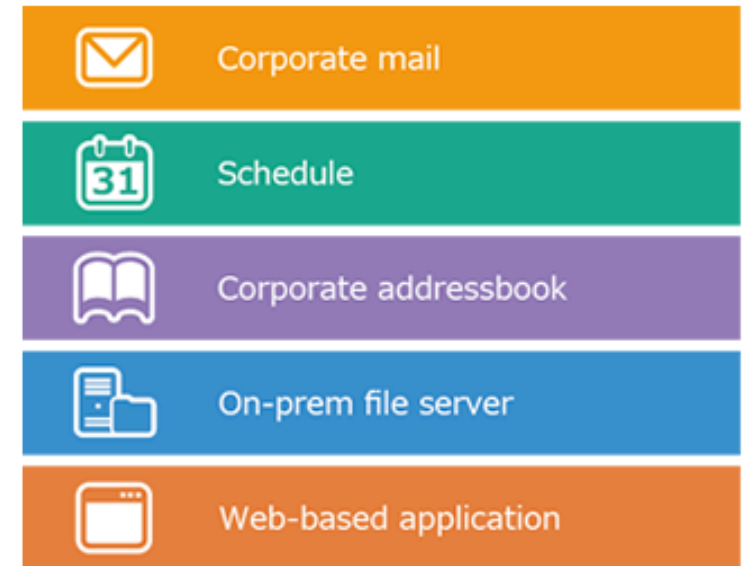
CACHATTO provides identity-centric network connection, providing authorised resources to the authenticated user, while all unauthorised resources are made invisible - reducing attack surface.

- Users are given access to authorised resources only
- Provides a permit-deny access control, rendering unauthorised resources inaccessible to users

Resource allocation

Managing CACHATTO and its users can be set within the corporate network. Allows precise access control to cloud environments, managing cloud-based resources

- Email
- Calendar
- File server
- Web-based system
- Cloud-based system
- Microsoft Teams



What is CACHATTO?

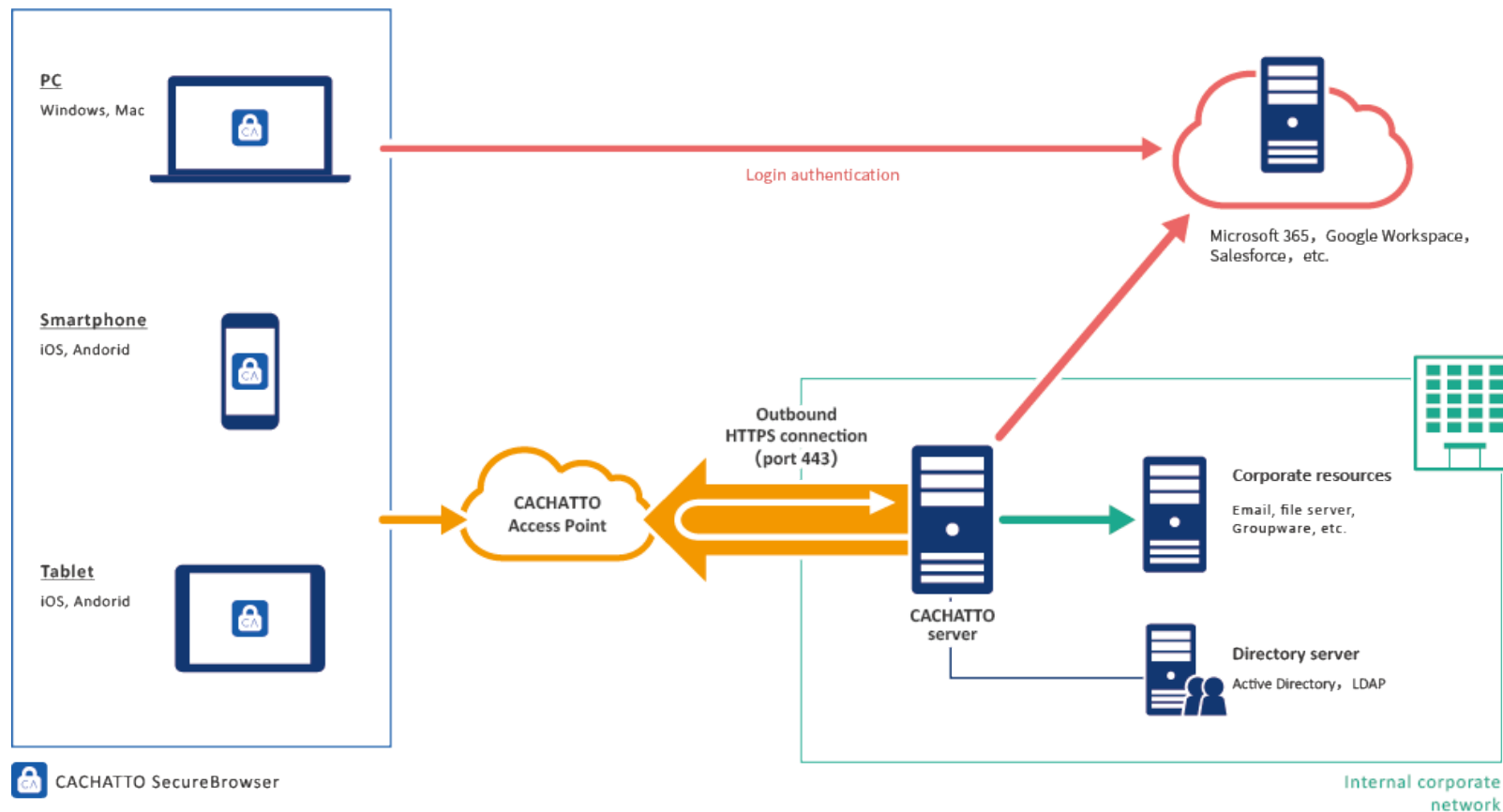
Supported resources

Supported applications and server	
Cloud-based groupware	Microsoft 365 (Exchange online) Google Workspace SharePoint Online
Web based groupware	desknet's Neo Cybozu Office Cybozu Garoon INSUITE AgileWorks POWEREGG Box EasyPortal
Groupware server	Notes/Domino Microsoft Exchange
Mail servers	POP3/APOP supported servers IMAP4 supported servers
File server browse	Windows server NAS
Instant messaging	Microsoft Teams

CACHATTO architecture

On-premise

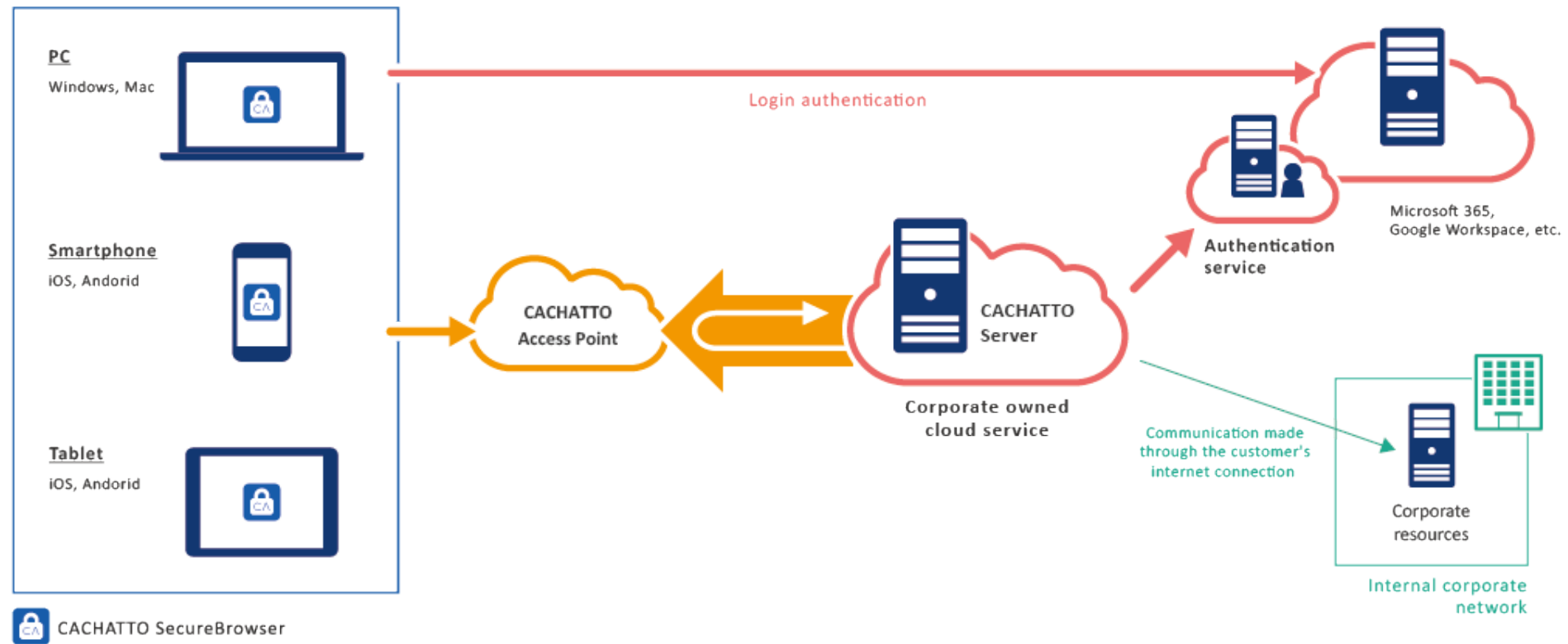
A CACHATTO server is placed within the corporate network. Implementation does not require any server in the DMZ or any inbound port, VPN nor changes to firewall settings are necessary; flexible and adaptable.



CACHATTO architecture

Cloud-based

CACHATTO can be deployed in the corporate owned cloud that can connect to the customers internal corporate network.



Providing 3 remote access solutions

Addressing the clients' needs

Providing the most appropriate solution for the customers

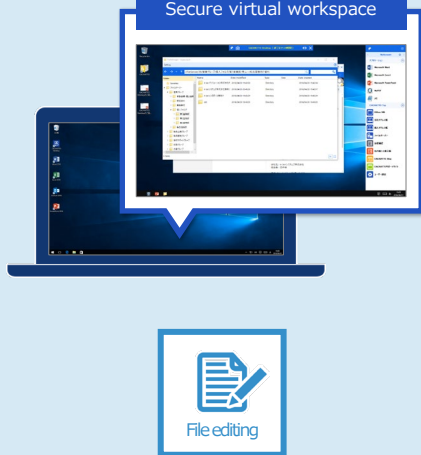
CACHATTO®
SecureBrowser



Remote access to corporate resources
via **SecureBrowser**

CACHATTO®
Desktop

Secure virtual workspace



Remote access to corporate resources
via **Sandbox environment**

splashtop®
for **CACHATTO®**



Secure and manageable
Remote desktop solution

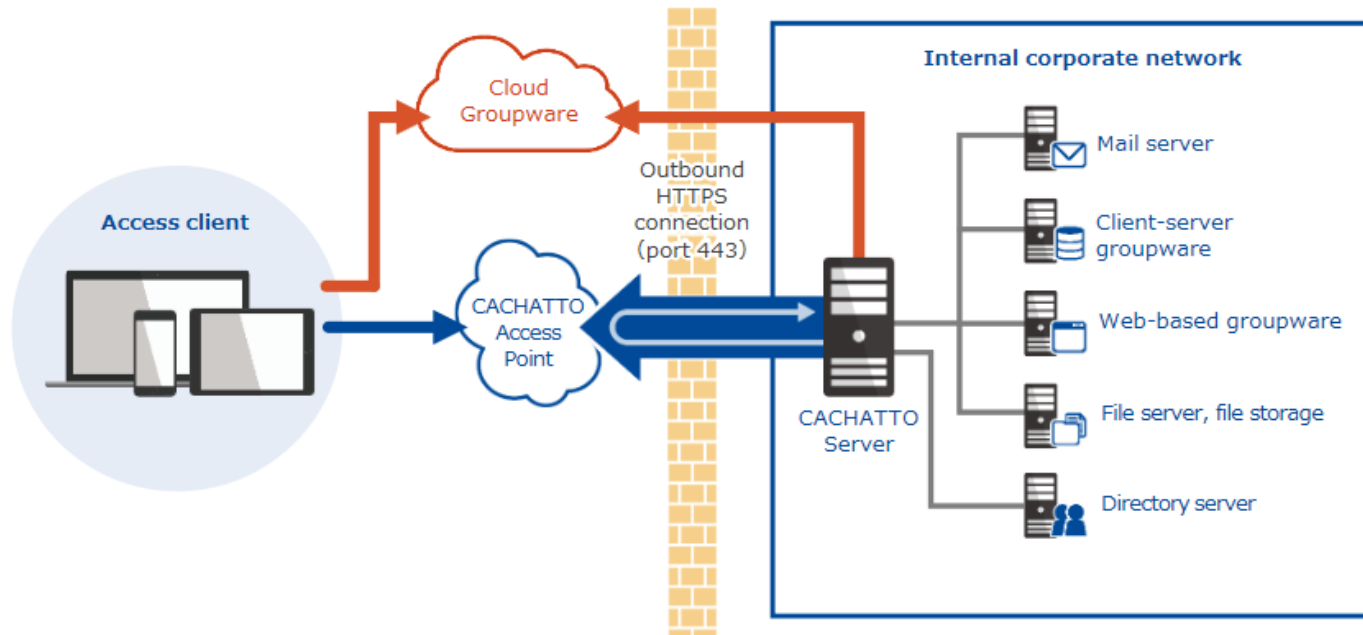
Feature of CACHATTO

Reduced surface attack

With CACHATTO's unique architecture, accessing clients does not have a direct access to the internal corporate network or resources, preventing possibility of lateral "east/west" attacks.

Servers and applications are isolated from clients, making resources hidden.

CACHATTO does not require changes in the firewall settings, VPN, inbound ports not global DNS; it only utilizes port 443, Outbound HTTPS connection, simplifying deployment while keeping system secure.

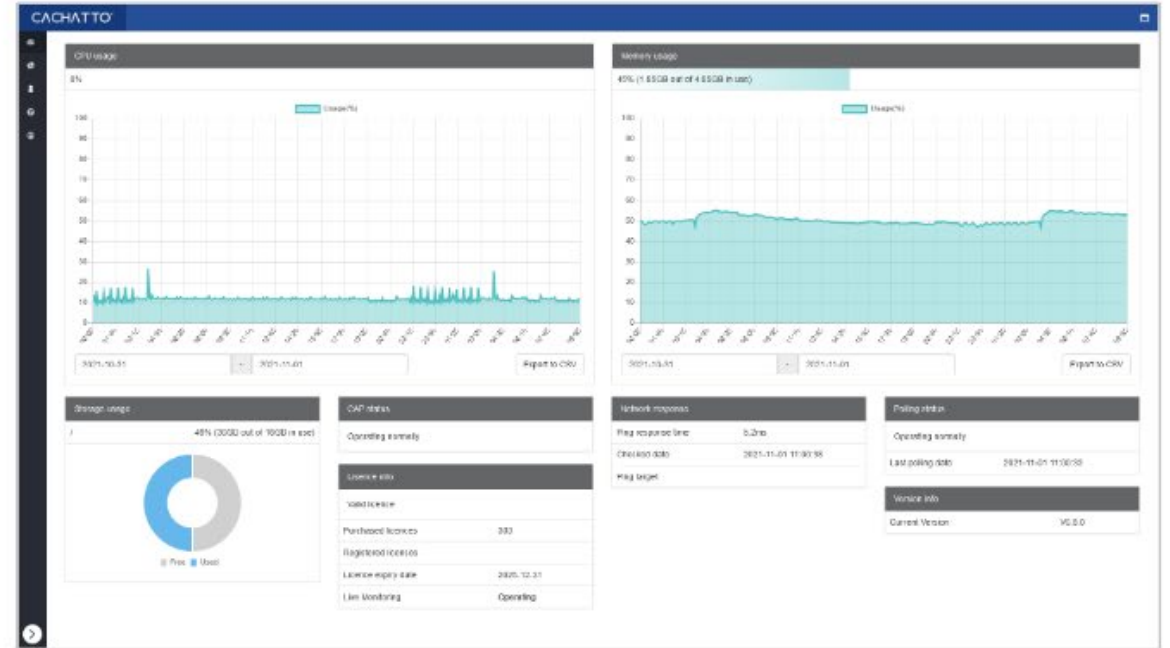


Features of CACHATTO

Registration and management

CACHATTO Administrator page enables registered administrators to set, manage and operate access restrictions, like various unique CACHATTO MDM functions, user and device settings, email and application settings, etc.

Administrator can also view access audit and CACHATTO's "Dashboard" function, which enables administrators to view and check information concerning the operating conditions of the CACHATTO server, user login, OS in use and CACHATTO version.



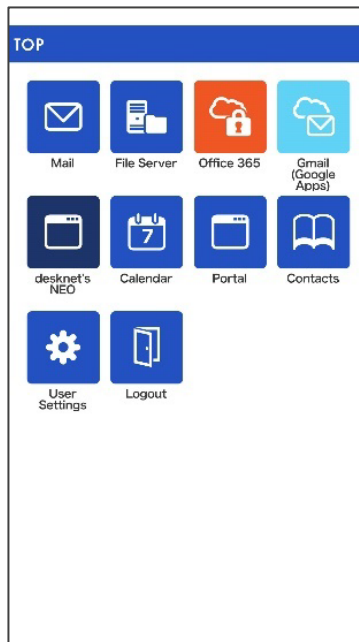
Features of CACHATTO

Security policy configurations and individualized resource allocation

CACHATTO security policies can be set on each individual accounts or by groups. This also includes CACHATTO's unique MDM policy settings, accessed corporate system restrictions, etc.

The administrator can activate, deactivate or delete a given user's account via the Administrator page.

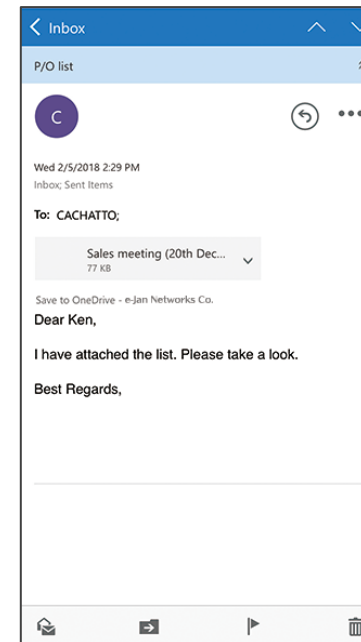
Moreover, administrator can individually customize users access to corporate system. This provides a easy to manage access control , rendering unauthorised resources invisible to the specific user.



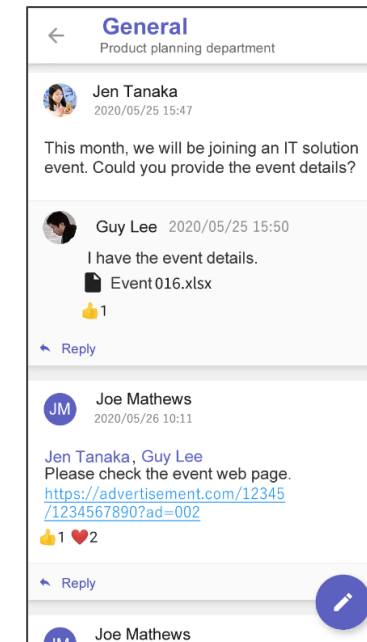
TOP page



Group calendar



OWA



Microsoft Teams integration

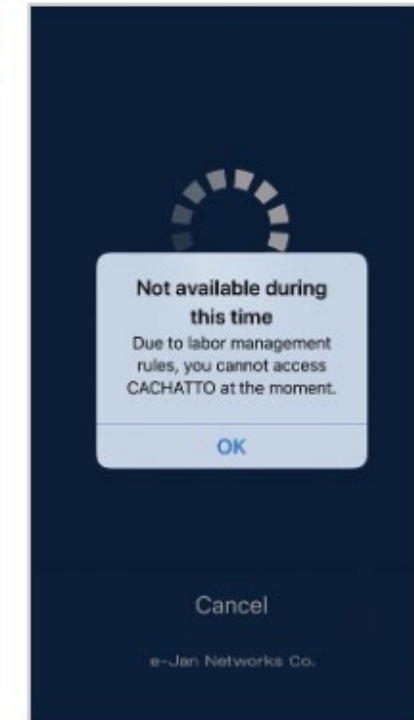
Features of CACHATTO

Labour management function

Labour management function enables administrators to set the hours, days of the week, which the user can log in to CACHATTO application. If user tries to log in during the set off-hours, a pop-up message will appear notifying the user.

The administrator may provide a “emergency use” option to the user.

The screenshot shows the CACHATTO web interface with the 'Group Policy Settings' page. The left sidebar contains a menu with 'Admin Settings' selected. The main content area is divided into sections: 'Group Policy Settings' (with fields for Group Policy ID and Group Policy Name), 'Labor Management Settings - PC' (with a table for selecting login hours for each day of the week), 'Labor Management Settings - Mobile/Android, Mobile, Android feature phone' (with a checkbox for 'Use the same settings as in "Labor Management Settings - PC"'), and 'Apply PC policy to tablet/...' (with a dropdown menu). The 'Labor Management Settings - PC' section includes a table with columns for days of the week and time slots, and an 'Apply to all' button.

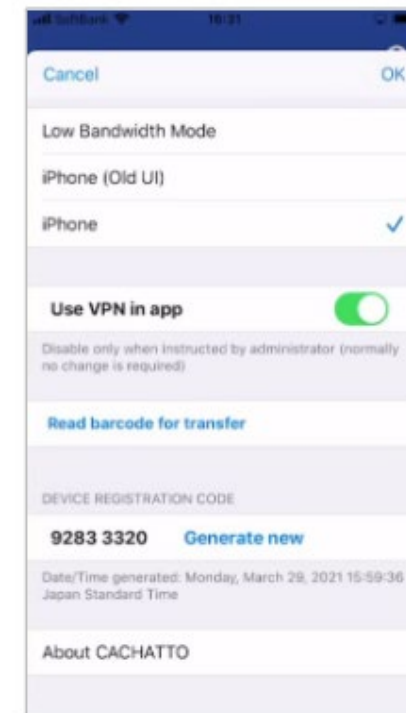
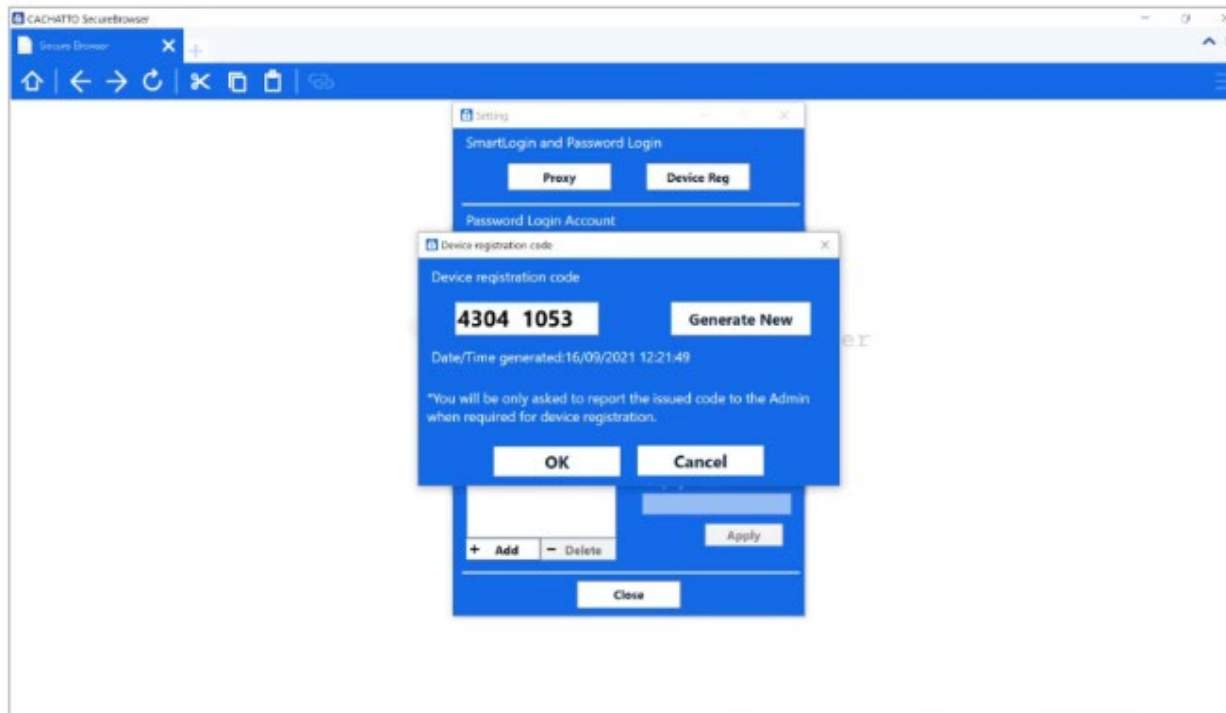


Features of CACHATTO

Device authentication

Device authentication is an authentication method that checks the specific device used by a given user account. This function prevents unregistered devices to access CACHATTO by authenticating the device used at the time of login.

Each User ID can register 1 to 4 devices by the discretion of the administrator.



What is CACHATTO?

User registration and configurations

Users can be registered individually or by bulk for easy registration. Each user can be customized individually with various settings like security policies, device usage, resource access, etc.

Administrator can activate, deactivate or delete users, even set an expiration date for a user account. Each User ID can register 1 to 4 devices by the discretion of the administrator.

Audit and Backup

Administrator can view access logs, including user, administrator, connection status, and other access logs. CACHATTO also provides the administrator to backup CACHATTO user data and settings information

Administrator notifications

Administrator can send notification messages to its users. This function also includes a way to send temporary passwords to users who are having trouble with CACHATTO access.



CACHATTO

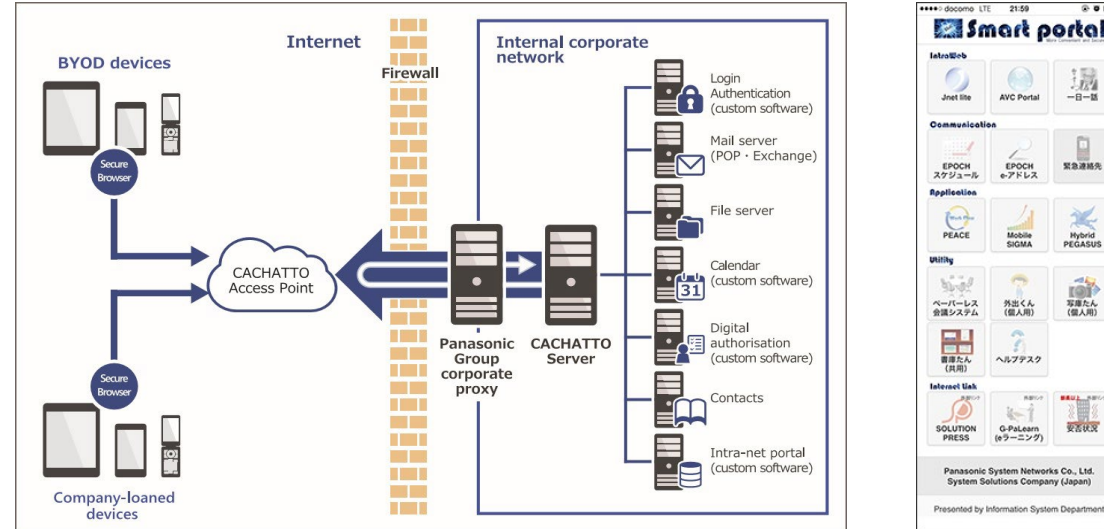
Client testimonies

Client testimonials

Panasonic System Solutions Japan

General Manager, Mr. Fuji, explained about why CACHATTO.

- Safety by not having a direct-access route
- Not needing to change the firewall settings
- Functionality - mail-display function, the multi-task feature, mobile phone interface
- Case studies on the use of CACHATTO by other companies and government offices which have high standards for security greatly influenced our product selection



*CACHATTO website client page (English): <https://www.cachatto.com/en/client/panasonic.html>

Client testimonials

Nippon Life Insurance Company (Nissay)

Nippon Life Insurance Company is one of the largest insurance companies in the world with 12 Million policies with \$650 Billion in assets.

Why CACHATTO:

- Security – *“Not only email text, but also attached files could not be saved to terminals, nor could they be brought out.”*
- Multi device support – hardware/platform agnostic
- Enables BYOD

What's next:

- *‘About three years have passed since CACHATTO was introduced. Thinking highly of the fact that no security incident has occurred, the head office has decided to expand the users of CACHATTO’*
- Considering deploying CACHATTO Desktop for telecommuting. Dropped VDI as it is very expensive and complicated

CACHATTO

Product and contact information

Product website

CACHATTO product information site

<https://www.cachatto.com/en/>

CACHATTO free trial

Contact and send an application for a 2 weeks free trial for 5 users by contacting out sales department or partner vendors

