Remote Access Platform

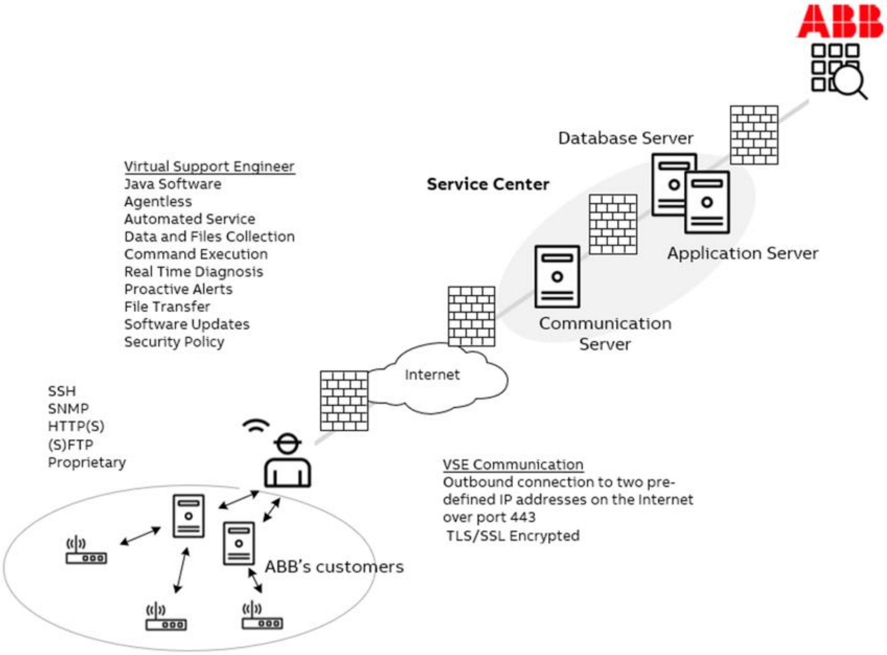
Architecture and Security Overview

Table of Contents

Overview

Solving a problem quickly and effectively from a remote location while providing a customer with excellent personal attention is a goal which can be difficult. In today's technological world, when a vendor or service provider supporting a mission critical application requires remote access, they often encounter substantial objections. Information Security Officers are faced with the dilemma of keeping networks secure and at the same time receiving vital remote support.

ABB has deployed new technology which provides the most innovative remote support offering in the industry. ABB's Remote Access Platform (RAP) was deployed in 2009 as the standard method used to provide remote support, as well as continuous remote monitoring and diagnostics. RAP security features address the concerns of IT administrators on security issues that surround remote support technologies. This document describes the security aspects of the solution.



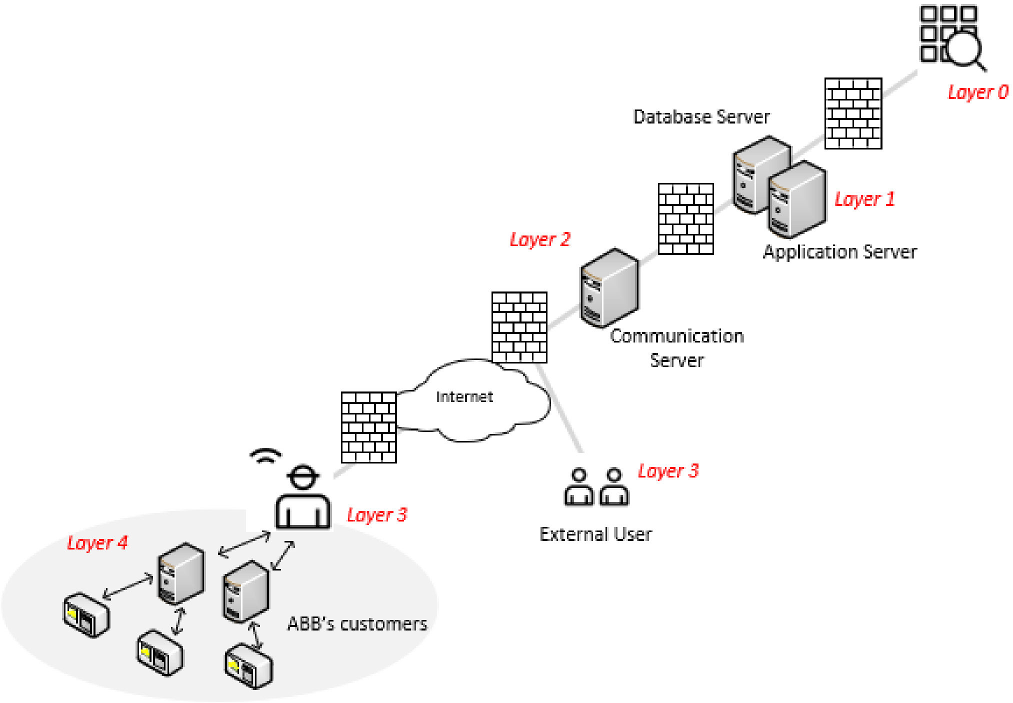
Architectural overview

With RAP, ABB securely deploys remote support to equipment installed behind customer firewalls. This solution has been designed for high performance and security at every level of its architecture. It securely communicates over the Internet and links ABB equipment to a central server at ABB. Through the RAP, your equipment can now provide performance data, alerts, and alarms to our support team so that we can deliver proactive, rapid service and support with advanced remote troubleshooting capabilities. Below is a technical description of this solution.

Remote Access Platform (RAP)

The ABB Remote Access Platform provides a secure connection to the site that is configured to meet all IT and regulatory security requirements.

Solution Architecture



Security layers overview

Remote Access Platform consists of five layers:

- Layer 0: Users launch the Service Center User Interface in the Web Browser
- Layer 1: Application and Database Servers residing in DB DMZ
- Layer 2: Communication Server residing in Web DMZ (accessible from Internet)
- Layer 3: Virtual Support Engineer (VSE) residing at client's facility (behind firewalls) and external users connecting to the Service Center from Internet
- Layer 4: Logical devices monitored by VSE (servers with software monitoring on-field devices connected to them by Optical links, Bluetooth, etc., or with other software where performance should be checked by VSE)

Solution Overview

- Application and database servers host the Service Center – This is a web application server that functions as the core of the system, acting as knowledge repository, control center and communication hub.
- Communication Server – Provides secure connection between VSEs and the Service Center.
- Virtual Support Engineer – Java software application located at the customer facility, which monitors supported devices and systems.
- Device – An instance of Product Line (PL) defined in VSE. May stand for PC where software supervising field device is deployed. Product Line is defined by ABB on the Service Center and represents the homogenous group (family) of devices. PL enables the VSE to collect data or perform various activities on devices defined at the customer site (in the VSE).

Before connection to Service Center can be established:

- Service Center definition must be added in the VSE
- Registration file of VSE must be delivered to the Service Center to define this VSE and import its fingerprint to the Communication Server. The fingerprint is unique for each VSE installation and securely stored on the VSE machine.

Every time the VSE exchanges data with the Service Center, it is through the secure TLS/SSL-encrypted tunnel, which is established after authentication of the server-side X.509 certificate and client – side fingerprint.

Description of Security settings

Layer 0:

- Users access the Service Center over https. Only a selected group of users, previously registered in the Service Center, can access the application. Privileges are granular. More detailed description can be found in Service Center User management section.

Layer 1:

- Communication between the Application server and the Communication Server is TLS/SSL-encrypted and each time it is initialized by the Application Server.
- Only messages coming from the previously registered VSEs are retrieved from the Communication Server. VSE registration records include the VSE's fingerprint (a piece of data computed on the VSE which is unique for every VSE).

Layer 2:

- Communication between the Communication Server and VSEs is TLS/SSL- encrypted with server-side certificate.

Layer 3:

- VSE can only communicate with the Communication Server whose public X.509 certificate is signed by a certificate authority which is trusted by the VSE through initial configuration.
- Communication is TLS/SSL-encrypted
- Communication is outbound only (i.e. VSE initiates the HTTPS session) with the VSE frequently polling the server for pending connection requests from users.
- All data gathered by the VSE can be browsed from the VSE Web User Interface and can be sent manually to the Service Center operator when needed.
- Users connecting to the external interface of the Service Center require an X.509 personal certificate issued by ABB and installed on their computer. It is verified by the server before the login screen to the Service Center displays. Communication is TLS/SSL – encrypted.

Layer 4:

- All Remote Activities are logged on in the VSE, as well as, in the Service Center.
- VNC remote desktop sharing sessions can be video recorded. The file is then saved on the VSE, as well as, on the Service Center.
- Security Policy – Every activity supported by the VSE can be given one of the following permission statuses: Allowed, Forbidden, Requires Approval. More detailed description can be found in Security Configuration of the VSE - Security Policy section.
- Each remote access session can be terminated by the VSE administrator.

Service Center User management

The Service Center administrator sets granular privileges for support engineers to use RAP. The system uses a role-based access control schema to assign permissions. User permissions vary according to the user's role. Roles are assigned to users per site, i.e. access control is not only granular to the level or privileges, but also limits the scope of the privileges to a given site.

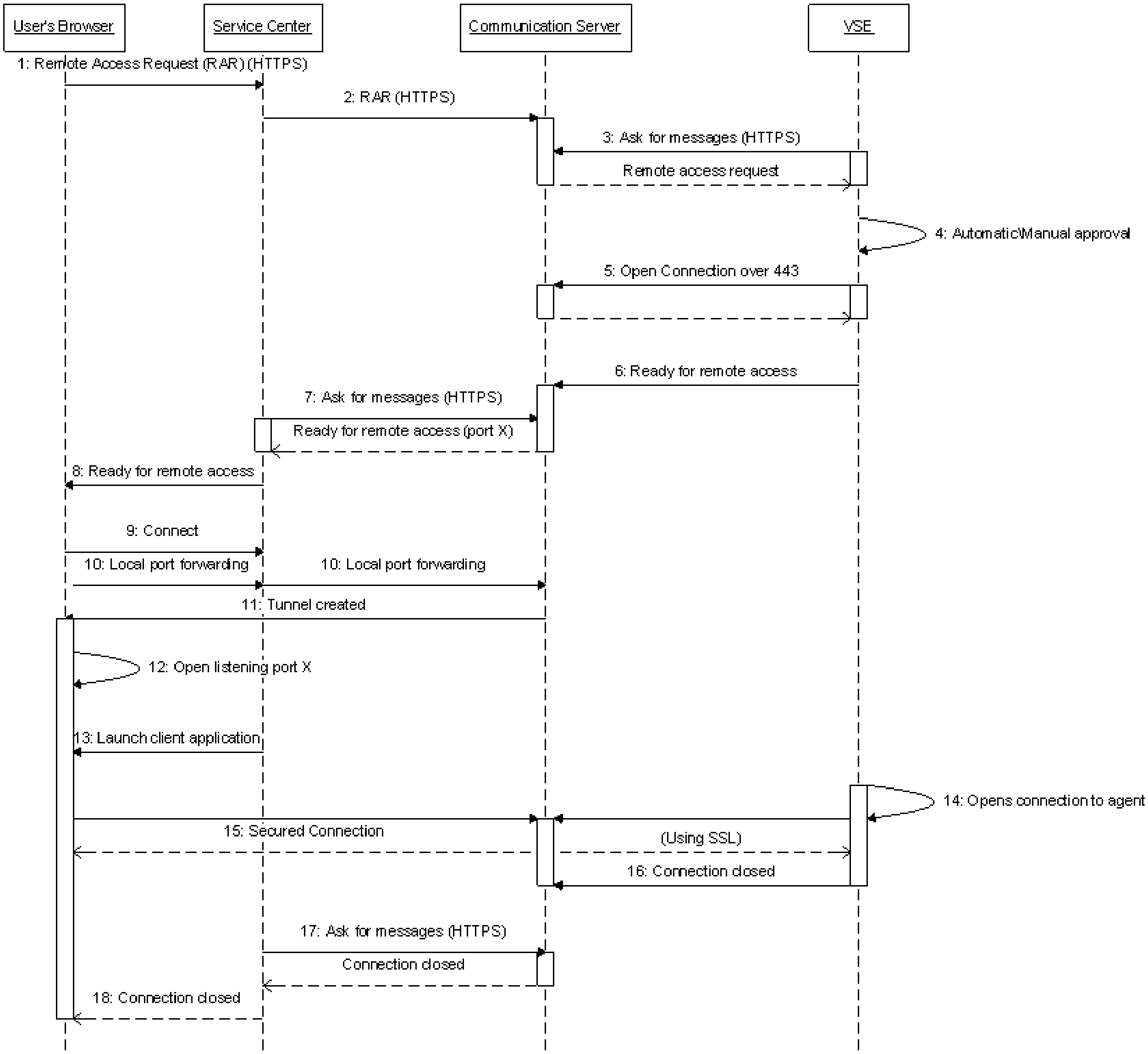
There are five roles in the Service Center:

- Administrators - manage VSEs install base and grant access to internal and external users from Service Center Administration Portal
- Group managers – user with administrative privileges within the specified site group.
- Operators:
  - Viewer – user who can only view the reports coming from the site.
  - Distributing Operator – user who also has the possibility to distribute software to the site.
  - Site Manager – user who has the additional privilege to perform all remote activities on the site.

Only users with administrative privileges can add new users to the application and register VSEs. Users with one of the Operator's roles cannot change their privileges or perform any administrative tasks.

Access to the Service Center must be requested by the RAP Regional Managers or Local group Administrators. Permissions to access individual plants or to operate specific commands on given assets are decided locally and dependent on contracts signed with the end customers. Connections from Service Center to the customer premises are also regulated by customers. They can deny or stop such connection at any time as described in Security Configurations of the VSE - Security Policy section.

Typical Remote Access Workflow


User's Browser
Service Center
Communication Server
VSE
1: Remote Access Request (RAR) (HTTPS)
2: RAR (HTTPS)
3: Ask for messages (HTTPS)
Remote access request
4: Automatic\Manual approval
5: Open Connection over 443
6: Ready for remote access
7: Ask for messages (HTTPS)
Ready for remote access (port X)
8: Ready for remote access
9: Connect
10: Local port forwarding
10: Local port forwarding
11: Tunnel created
12: Open listening port X
13: Launch client application
14: Opens connection to agent
15: Secured Connection
(Using SSL)
16: Connection closed
17: Ask for messages (HTTPS)
Connection closed
18: Connection closed

Communication workflow overview

When the support engineer gains Secure Remote Access to one of the units from his desktop, the system creates a remote access task request on the Service Center (1), filling it with all the appropriate parameters defined by the user. (2) The request is then placed on the Communication Server using HTTPS protocol. (3) The appropriate VSE polls the Communication Server for new messages every predefined number of minutes using HTTPS protocol. The new request is retrieved. (4) Depending on the current VSE configuration, the following occurs:

- Manual approval: the system sends an email to the local system administrator requesting his approval for the remote access. The administrator can click on the link in the email to view the request details.
- Automatic approval: the remote access is automatically granted for the period requested.

(5) VSE opens an outgoing, encrypted, TLS/SSL connection over port 443 to the Communication Server.(6) Once the secured connection is established, VSE sends a message to the Service Center (using HTTPS) acknowledging that it is ready for remote access. (7) The Service Center polls the

Communication server and receives the notification that the new tunnel has been established on port X (port X is chosen from list of available ports). (8) The Service Center sets the remote access request to the “ready” status. (9) The engineer is getting his remote connection initiated, (10) which implies the request to the Communication Server for the local port forwarding. (11) The Communication Server creates SSH tunnel to the User’s computer. (12) Local forwarding client downloaded from the Service Center on the user’s computer opens a listening port X to be used by the engineer-side client in the remote access. (13) The Service Center launches the appropriate client application on user’s computer. For example, in the case of desktop control a VNC client is launched with a live connection to the unit. (14) The VSE opens a connection to the appropriate agent on the unit case using the appropriate protocol (for example the VNC agent in the desktop control). (15) All the data flows between the VNC server and the VNC client through the established secured communication channel (over TLS/SSL). (16) When the predefined session time has elapsed, the VSE closes the connection and notifies the Service Center. (17) The Communication Server detects that the session has been terminated by the Virtual Support Engineer and closes the listener socket. (18) When Service Center recognizes that the connection has been closed – closes the client application.

Security Configurations of the VSE

The core component of the Remote Access Platform is the Virtual Support Engineer (VSE) - a small footprint Java application that is deployed at the customer site to monitor and maintain availability and health of ABB software and/or hardware 24/7. This Virtual Support Engineer is the hub of RAP executing all necessary support commands and communication from the supported customer site to the support provider.

The Virtual Support Engineer's security settings are completely controlled by the end customer's IT management at the customer site at which it resides. It is ABB's end customer who is granted control to set the security policies and communications to the remote support process. The Virtual Support Engineer checks the Communication Server situated at ABB to receive updated instructions for the automated support functions it must execute. For an automated self-healing action, the Virtual Support Engineer will establish a remote access session directly to the device it supports.

Communication Methods

VSE can communicate to the Service Center using one of the communication methods:

- HTTPS – encrypted connection via Communication Server (default option). Only this option allows Remote Access activities.
- Manual – offline method. Data transfer between Service Center and VSE must be done manually (e.g., the use of USB).

Additionally, from the Control Panel in the VSE User interface – it can be switched to the offline mode. Then, no data is transferred to the Service Center.

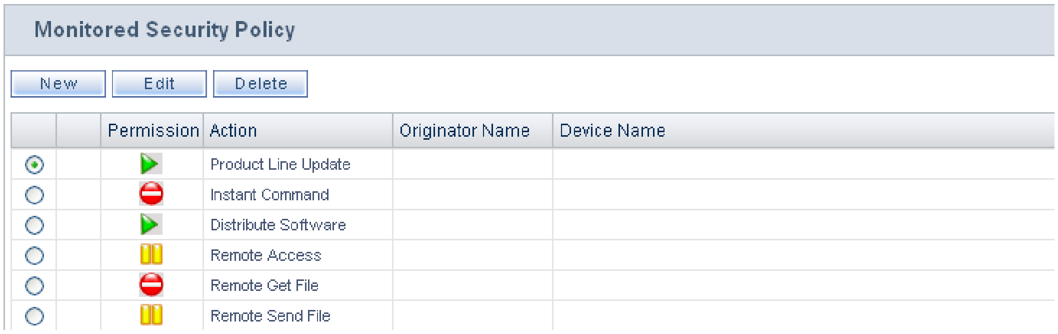
Security Policy

ABB gives the end customer full control over all communication between the onsite Virtual Support Engineer and the Communication Server, as well as, between the applications and devices which the Virtual Support Engineer monitors on the network. No matter whether these are simple Secure Shell sessions, desktop sharing activations, remote upgrades, or remote fixes, it is the end customer who determines the policies of the type of on-site actions that can occur. ABB is always reliant on their customer to authorize and allow any remote access session (automatically based on rules or manually for each individual session), and to set policies to control what information is accessible and which tasks can be performed by the Virtual Support Engineer. To determine these policies, the end customer can configure permissions in the Virtual Support Engineer which allow certain routines to run. These routines may require the Virtual Support Engineer to send the end customer's plant operator an email requesting permission to execute the requested task.

The VSE UI enables VSE administrator to define permissions and actions that are conditioned by rules. Each task performed by VSE on the request from Service Center can be given one of the following permission statuses:

- ▶ Allowed,
- ⛔ Forbidden,
- ⏸ Requires approval.

The Monitored Security Policy screen displays a list of policy rules currently defined in the system in the order in which they are handled by VSE. The top line displays the rule with the highest priority. The list continues in descending order. VSE allows the administrator to change the priority of an existing policy rule.



		Permission	Action	Originator Name	Device Name
●		▶	Product Line Update		
○		⛔	Instant Command		
○		▶	Distribute Software		
○		⏸	Remote Access		
○		⛔	Remote Get File		
○		⏸	Remote Send File		

Local RAP permission settings

The rules matching process is subject to two conditions:

- VSE processes the rules as they appear on the Monitored Security Policy screen in descending order.
- VSE exits the policy management routine immediately when it finds a rule which matches.

If no policy rules are defined, all pending (Remote Activities) will be assigned the state “Waiting for Approval”. The VSE administrator must manually approve each remote activity individually.

Detailed log trails

All data sent from or received by the Virtual Support Engineer are logged automatically and recorded in operational and audit logs. This makes it easy to view any past service event. As a remote support session is initiated, all data transfers are logged including the applications and devices involved, as well as, the usernames of support engineers to provide a detailed audit trail of information. Traceability is maintained on Service Center side and the VSE side. All remote secure shell sessions are automatically logged and stored for future reference. VNC sessions can be screen (video) - recorded and then the record is available on Service Center and the VSE.

The VSE Audit Log stores a list of all user-initiated activities performed at the VSE. These activities include configuration changes at the site. An audit message is written to the Audit Log of the VSE. The log is displayed as a table with the following columns:

- Severity
- User - under what user the event was logged
- User Type (local or remote)
- Message - the event message (like “Remote Connection to the device <device IP> has been established.”)
- Time Generated - when the event was generated
- Device IP (localhost for the VSE machine)
- Device name – the name visible in the device list

Similar entries can be found in the Service Center audit log. Additionally, on both ends, there are logs devoted only to remote activities with the following columns:

- Status – the status of the activity (Requested, Waiting for Approval, Executing, Finished)
- Submit/Arrival Date
- Last Status Change
- Submitted/ Requested by – the username who created the remote activity
- Activity type and application used
- Brief
- Completed

Remote Connections management

Each remote session may require approval from the VSE administrator depending on the security policy. Additionally, VNC sessions can be screen (video) - recorded and then the record is stored on both ends – on VSE as well as in the Service Center. VNC sessions can also be supervised by the VSE administrator, while the SSH sessions can be viewed during its execution time.

If required, each remote connection can be terminated by the VSE administrator without notifying the remote user. Then, the remote connection is terminated immediately. Termination of remote sessions is done via the VSE UI, which is accessible to all authenticated and authorized users on the same subnet as the VSE.

Connection to devices

Each field device supported by the VSE is represented in the database as a specific instance of the Product Line to which the device belongs. After the Service Center administrator sends a Product Line for a supported family of devices to the VSE, a device can be created in the VSE. The device definition includes the device Unique ID, IP address or computer name, hardware model, and software version. The device definition also includes the communication protocol settings.

Protocol settings

The protocol settings define how to communicate with the VSE for each protocol running on the device, including which ports to use for connecting to the device, and the required login parameters.

A choice of protocols VSE can work with:

- FTP (Secure FTP)
- SSH
- TL1
- WMI
- DMI
- SNMP
- Proprietary

If a firewall resides between VSE and monitored devices, appropriate ports (depending on the Product Line settings) need to be open to enable the communication between VSE and the device. Additionally, to enable remote access via:

- WinTerm – port 3389 and/ or VNC – port 5900
- Remote Browser – Depending on which port listens the remote application (installed on a device computer).
- SSH – Port 22 needs to be open on that firewall.

Application confidentiality

Upon deploying Virtual Support Engineer at the customer's sites, only the customer can set permissions for the devices, servers, and applications which the Virtual Support Engineer will monitor. These permissions provide username-password credentials for accessing the Virtual Support Engineer, as well as, each device and application that the Virtual Support Engineer will monitor. These credentials are never exposed to ABB and are encrypted before being stored on the Virtual Support Engineer.

Only the local authorized Virtual Support Engineer can communicate with devices on the monitored network. No device IP address is communicated during any remote access sessions.

Frequently Asked Questions

Q: What is the access control policy for the system?

A: RAP is based on the Least Privilege standard of practice.

Q: Who is the application owner (i.e. who can make the business decisions on who needs which level of access)?

A: Business decisions as to who needs which level of access are defined by Regional/Country RAP SCL Manager and/or by Local Group Administrators.

Q: What is the granularity of permissions that you need to be able to manage?

A: RAP Service Center (SC) is accessible by local BUs RAP Users. This access must be requested by the Regional RAP Managers or Local group Administrators. Permissions to access individual plants or to operate a specific command on a given asset are decided locally and dependent on BUs contracts signed with end customers. Connections from customer premises to RAP SC are also regulated by customers. Customers can deny or stop such connections at any time.

Q: Which levels of access are needed in the system?

A: ABB has RBAC in place. That means we split RAP ABB users into groups: Administrators, Group Administrators, Site Managers and Operators. And for each user the access to each remote access action can be granted/restricted.

Q: What changes to the firewall are needed to prepare the VSE installation on the site?

A: The best practice is to install VSE in the same subnet as the computers hosting the systems to be monitored (logical devices). Then, the only change will be needed on the firewalls routing the connection from the VSE computer to the Internet. Enable communication over port 443 to two predefined IP address - outbound only.

In the case when VSE is separated by the firewall from the logical devices, the standard set of ports includes 3389 (WinTerm) and/ or 5900 (VNC), 22 (SSH). The other ports to be opened depend on the kind of monitoring to be performed.

Q: What if ABB already has established remote service with a customer using dial-up and remote desktop software like PC Anywhere?

A: For customers that have dial-up remote service, we want to switch them over to ABB's Remote Access Platform. Usage of RAP makes it easier to manage sessions, log connections, provide secure connections, and perform data transfer. For instance, ABB can provide a video capture of any VNC remote desktop session and save it to a flash file. Additionally, a broadband connection via the Internet provides more accessibility by ABB and is a much faster interface.

Document Change Control

Author	Revision	Date	Description
Karolina Zarawska	Initial		
Karolina Zarawska	A		
Karolina Zarawska	B	03/07/12	
Patrik Boo	C	06/24/14	New template.
Laurentiu Manole	D	06/22/21	Document review and update