TrustVisitor

Pre-Installation Guide

Version 1.0.0

Last Updated: January 2024

For use with TrustVisitor 4.1.1

Table of Contents

Version Control

Version identification is a simple integer sequencing at each level following the format X.Y.Z where X is the version, Y is the sub-version, and Z is the draft level (ex. v1.0.1).

Version: A new release of this document which has a significant change that requires a change in the operating process or procedures.

Sub-version: A new release of this document which has no significant changes and does not require a change in the operating process or procedures.

Draft: Draft versions are for internal use only for authoring changes.

On its effective date, a formal version of this document becomes available for distribution. New versions of this document supersede all previous versions.

Version	Effective Date	Summary of Changes
1.0.0	01/2024	TrustVisitor v4.1.1

About TrustVisitor

TrustVisitor is a state-of-the-art enterprise visitor management platform designed for organizations using advanced authentication methods. You can create events via email and invite Visitors internal or external to the organization. Visitors who need physical access authorization can register via email, gain the required approvals, and seamlessly gain the appropriate access.

This guide describes how to install TrustVisitor. Use this guide to plan your TrustVisitor implementation and gather the information you'll need prior to installation.

TrustVisitor Background

TrustVisitor is a high-assurance visitor management solution. Understanding the key concepts of TrustVisitor is crucial to a smooth installation and configuration process.

TrustVisitor Roles

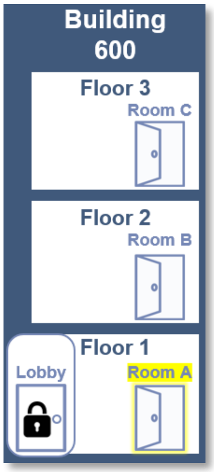
There are five roles associated with common TrustVisitor meeting tasks, such as creating a meeting, inviting individuals who need building access authorization, and granting access to the facility at the appropriate time:

- **Sponsor** – Sends a meeting invitation email.
- **Visitor** (Meeting Invitee) – Responds to the meeting invitation email and provides information for access approval.
- **Security Officer** – Performs a security check on the Visitor, if required for the meeting location.
- **Approver** – Finalizes access permission for the meeting location, if required.
- **Lobby Guard** – Upon Visitor arrival at the facility, reviews Visitor request for completeness, grants building access, and issues a temporary credential, if required.

Meeting Locations

For TrustVisitor to assign access to Visitors in the PACS for an Event, it must know which PACS access location(s) control access to the Event Location.

When a Sponsor sends a meeting invitation, they don't use PACS locations; they use Active Directory (AD) locations (i.e., Rooms). TrustVisitor translates an AD location into a PACS location or sequence of locations). This is accomplished with a hierarchy in TrustVisitor that mirrors your organization's Region, Campus, Building, Floor, and Room configuration. You don't have to replicate every physical location in your environment, only the locations a Visitor might need to access.



Location Example 1

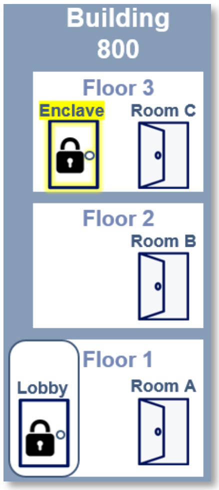
Sponsor Bob invites Visitor Alice to a meeting located in **Room A** in **Building 600**.

In TrustVisitor, the AD location **Room A** is paired with the PACS access location **Floor1-RoomA**. The location **Room A** is inside the location **Building 600**.

When Alice arrives in the **Building 600** lobby for the meeting, she will receive an assigned Visitor badge. The badge must be provisioned in the PACS to include all required locations between the lobby and the meeting location.

In this example, the location is **Building600Lobby** as that's the only PACS location for this building.

Location Example 2



Sponsor Alice invites Visitor Bob to a meeting in the **Enclave** on February 1 from 10AM to 11AM.

In TrustVisitor, the AD location **Enclave** is paired with the PACS access location **Floor3-Secure-Enclave**. The location **Enclave** is inside the location **Building 800**.

When Bob arrives in the **Building 800** lobby for the meeting, he will use the same PIV card he used for Visitor registration to access the meeting location. At 9:45AM, TrustVisitor sends Bob's PIV card information to the PACS and provisions the access locations **Building800-Lobby** and **Floor3-Secure-Enclave**. Bob uses his PIV card, attends the meeting, and leaves when the meeting ends. At 11:15AM, TrustVisitor removes Bob's PIV card from the PACS.

By default, TrustVisitor assigns access 15 minutes before the start of an Event and removes access 15 minutes after the end of an Event. These are configurable values.

Access Control in TrustVisitor

TrustVisitor provides granular access control using Security Groups from your AD. You can provision global access to all of TrustVisitor, finite access to certain locations, and anything in between. This granularity applies to both software configuration and operations.

For each TrustVisitor location, you can use AD Security Groups to manage:

- Who is an authorized Sponsor (can invite Visitors to the location).
- Who is an authorized Security Approver.
- Who is an authorized Location Approver.
- Who is a valid Lobby Guard (can process Visitors upon arrival at the location).

You do not have to use unique Security Groups for each setting. For example, you can share Approvers across some locations (but not Lobby Guards) or use one Security Group for multiple locations.

Architecture and Platform

TrustVisitor is based on a Microsoft Windows Server environment. TrustVisitor is installed on a domain-joined machine to take advantage of higher security Integrated Windows Authentication. You can install services on a single all-in-one server or on multiple servers with role-based separation.

TrustVisitor Components

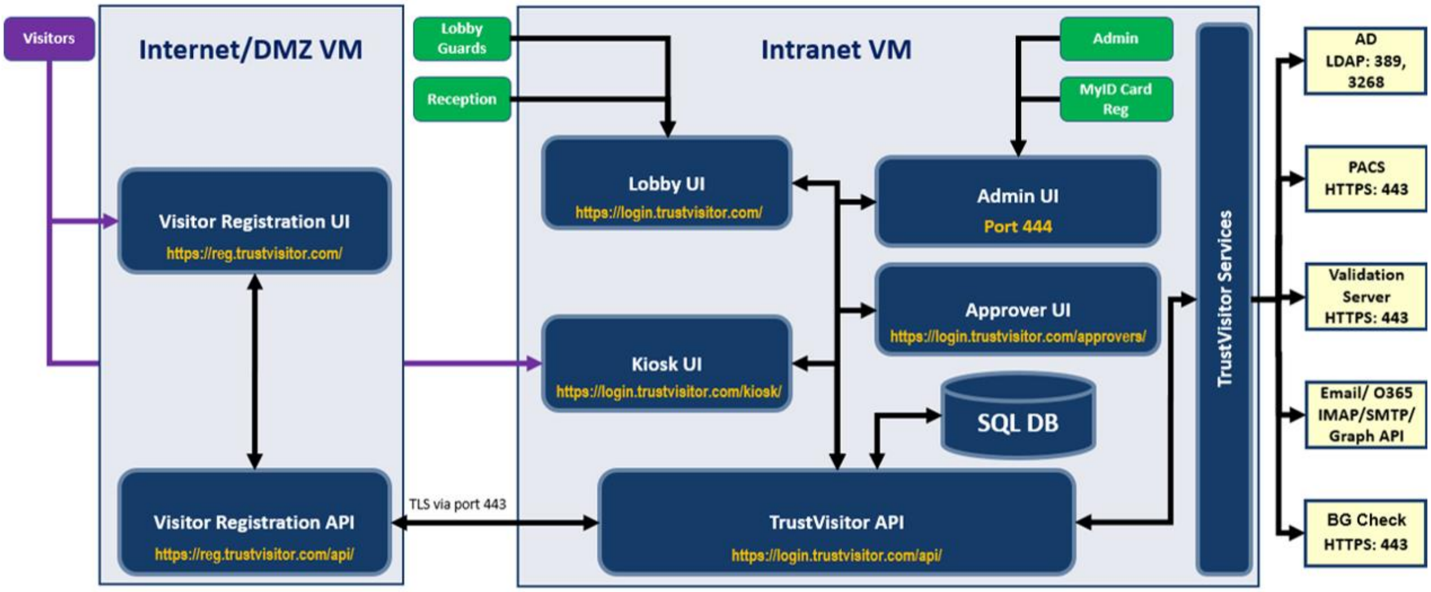
TrustVisitor comprises the following parts:

Component	Description
TrustVisitor Lobby/Admin Applications *(Hosted in Microsoft IIS)*	Privileged web interface for managing Visitors and Events and assigning badges to personnel. Internal access only with integrated smart card logon; requires a valid SSL certificate issued to the host.

Component	Description
TrustVisitor Visitor Registration	Public web interface used by Visitors to register for meetings in advance. Must be internet accessible and issued a valid SSL certificate.
TrustVisitor Background Service Applications	Privileged applications that provide background syncing between LDAP, SQL, Mail, and the PACS.
Microsoft SQL Server	SQL Server 2019 Standard Edition (or later), OR SQL Server 2016 SP1 Enterprise edition is required as it includes built-in encryption tools. TrustVisitor can integrate with an existing SQL Server database.
Microsoft Active Directory Domain	User authentication and permissions. TrustVisitor typically integrates with an existing AD domain.
Email Server Access	TrustVisitor utilizes mail for a variety of purposes. TrustVisitor typically integrates with an existing Exchange server or Office 365 deployment.
Internal Email Account	Monitored by TrustVisitor. Used for receiving meeting invites and interacting with Sponsors/Approvers. Also used to send system notifications and alerts.
Compatible PACS	Used for provisioning physical access to Visitors and Employees. Must perform proper certificate validation of credentials on a regular basis.
Workstation(s)	A physical workstation for operator and administration functions. Used to access web applications hosted on the Microsoft IIS server and must support use of a smart card reader, either USB or internal. Will have middleware applications installed to allow web services to interface with peripherals.
Peripheral Hardware *(Attached to the Workstation)*	ID Reader/Scanner with supporting software license (Acuant ID150 or Scanshell 800 DXN are recommended) Contact Card Reader RFID Reader: RFIdeas PCProx Plus Model: RDR-80081AKU Remote PIN Pad 7 Port Powered USB Hub (optional)
Credentials	Blank cardstock to be programmed.

TrustVisitor Conceptual Diagram

The following diagram shows a conceptual view of a production deployment of TrustVisitor. In this design, the Visitor Registration components are installed in an externally accessible VM while the rest of TrustVisitor is running on an internal VM.



All ports numbers shown are configurable

VM Deployment Suggestions

The following suggestions are minimum requirements. You may need to increase core count or memory/disk space for larger installations.

- DMZ Application/Web Server (Visitor Registration):
  - VM Configuration: 2 cores / 8GB memory / 64GB VHD
  - Operating System / Server Configuration:
    - Windows Server 2016 (or higher)
    - Microsoft IIS, .NET 6 (or higher)

- Internal Application/Web Server (Admin/Lobby):
  - VM Configuration: 2 cores / 8GB memory / 64GB VHD
  - Operating System / Server Configuration:
    - Windows Server 2016 (or higher)
    - Microsoft IIS, .NET (or higher)

- SQL Server:
    - VM Configuration: 2 cores / 8GB memory / 64GB VHD
    - Operating System / Server Configuration:
        - Windows Server 2016 (or higher)
        - SQL Server 2019+, Standard Edition, or SQL Server <2019, Enterprise edition

- Workstation:
    - Physical Hardware Configuration:
        - 2 cores / 8GB memory / 128GB HDD
    - Operating System / Server Configuration:
        - Domain Joined Windows 10 workstation
        - Current Java SE JRE installed
        - Windows Biometric Framework installed

TLS Certificates

The TrustVisitor solution requires TLS certificates to ensure secure communications traffic. These certificates are installed in Microsoft IIS Manager for each website as follows:

- A TLS certificate for each of the TrustVisitor websites.
    - The Visitor Registration application needs a TLS certificate trusted by all modern browsers. You should use a certificate issued by a known, trusted public Certificate Authority so any Visitor's browser can recognize the root CA. Examples of trusted CAs include DigiCert, GoDaddy, Symantec, Thawte, and VeriSign.
    - The Lobby application needs a TLS certificate trusted by all internal Employees (e.g., Guards, Approvers, etc.). This can be issued from an internal PKI, if one exists.
    - The Admin application needs a TLS certificate trusted by all internal Employees (e.g., Guards, Approvers, etc.). This can be the same certificate used for the Lobby application or a unique certificate if desired.
- The TrustVisitor installer prompts for the pfx certificate file (and password) to be used during installation. This can always be changed after the install completes using IIS Manager.
- A TLS certificate for client authentication of the TrustVisitor webserver to the PACS Validation Server (e.g., HID pivCLASS).

Each certificate should reflect the host FQDN in the SAN DNS attribute.

SQL Server Requirements

TrustVisitor uses Microsoft SQL Server as its database. You can install SQL Server on the Application Server (less common) or a separate server (more common). SQL Server 2019+, Standard Edition, or SQL Server <2019, Enterprise edition is preferred because of its encryption tools as it relates to protecting personally identifiable information (PII) that may be captured and stored by TrustVisitor.

If SQL Server is installed on a separate server, the TrustVisitor installation will require authorized Windows login with sysadmin privileges to a blank TrustVisitor database. These privileges can be reduced to read/write after installation.

The following two accounts are required for TrustVisitor installation:

- A Computer account of the TrustVisitor server; and
- A Windows account for the individual user installing the TrustVisitor application.

The following SQL Server Installation Features are required:

- Host is Domain Joined prior to install
- Database Engine
- Management Studio
- Client Tools Connectivity

Active Directory Requirements

TrustVisitor relies on the organization’s AD for queries, user authentication, and permissions.

TrustVisitor Roles

The following are the TrustVisitor roles that rely on AD Group membership:

- **Location Administrator:** AD Security Group that has the ability to make changes to an object in TrustVisitor. In general, they can make changes to the location but are not inherently given permission to assign credentials or provide access to users.
- **Location Operator:** AD Security Group that has the ability to see an object in TrustVisitor. Operators can manage Employees/perform reception tasks at a location.
- **Location Approvers:** AD Security Group that will receive notifications for and will have authority to approve visits.
- **Location Security Officers:** AD Security Group that will receive notifications for and will have authority to process Visitors for offline background/security screening prior to potential visit approval or access to the site for the specific location assigned. TrustVisitor allows the same AD Group to be used for multiple locations.
- **Lobby Guards:** AD Security Group of personnel that can check in approved Visitors at a site at the time of their meeting.
- **Employees Eligible to Return to Office:** AD Security Group of Employees who are designated to return to the office. Employees with this role may submit Employee Wellness Screening.

TrustVisitor distinguishes between Global and Local permissions. Global permissions apply across multiple locations, while Local permissions apply only to specific locations.

Security Groups

AD Security Groups are assigned to specific roles and permission sets. While it is not required, it is recommended that you create the following Security Groups for ease of distinction:

- TV Global Administrators

- TV Local Administrators
- TV Global Operators
- TV Local Operators
- TV Lobby Guards
- TV Employees Eligible to Return to Office

TrustVisitor roles may also be applied at the building level, with corresponding AD Security Groups. For example, if a building is designated “Corporate HQ,” the associated AD Security Groups would be:

- Corp-HQ Administrators
- Corp-HQ Operators
- Corp-HQ Receptionists
- Corp-HQ Visitor Approvers
- Corp-HQ Security Officers

TrustVisitor also uses Security Groups for user verification and email distribution of Approval and Security Officer related messages. TrustVisitor uses IIS integrated security for single sign-on pass through authentication. As a result, permissions within TrustVisitor are role based and rely exclusively on AD Group membership. For example, if you wish to provide access to process Visitors for Location33, Lobby Guards logging into TrustVisitor will need to have membership in the Security Group you’ve assigned to Location33’s Lobby Guard role.

TrustVisitor users cannot receive, view, or respond to approval or security requests if they are not members of the appropriate AD Security Group.

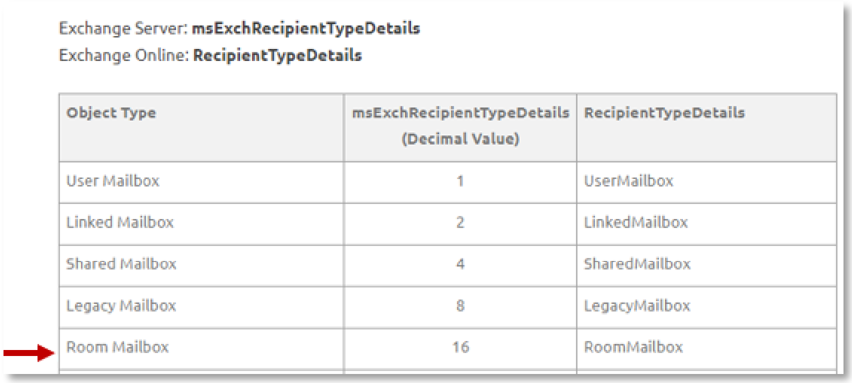
Meeting Locations

TrustVisitor relies on Microsoft Exchange/Office 365 and AD to recognize a location sent in a meeting invitation and provide the correct PACS access for the Event. In TrustVisitor, you can designate individual rooms as meeting locations or assign multiple AD locations to a single TrustVisitor location. TrustVisitor also supports a hierarchy, where you can specify the following locations:

- Region
- Campus
- Building
- Floor
- Room

TrustVisitor uses an attribute provided by Exchange to identify Room resources. In Exchange Server, set the *mxExchRecipientTypeDetails* attribute to 16. In Exchange Online (Office 365), set the *RecipientTypeDetails* to RoomMailbox.

If you use the Exchange interface (GUI or admin CLI) to create rooms, these attributes are set automatically. If you create the room resource manually in your AD, you will need to set these attributes. The following image shows the attribute information for both Exchange Server and Exchange Online.



Exchange Server: **msExchRecipientTypeDetails**
Exchange Online: **RecipientTypeDetails**

Object Type	msExchRecipientTypeDetails (Decimal Value)	RecipientTypeDetails
User Mailbox	1	UserMailbox
Linked Mailbox	2	LinkedMailbox
Shared Mailbox	4	SharedMailbox
Legacy Mailbox	8	LegacyMailbox
Room Mailbox	16	RoomMailbox

Mail Server Requirements

As part of its normal operations, TrustVisitor requires access to a mail environment to send and receive emails. You will need to create a mailbox for TrustVisitor in your mail environment so TrustVisitor can send messages to Visitors, Sponsors, and Approvers and process their replies. Sponsors invite the TrustVisitor email address to any meeting invitations that require Visitor processing. The TrustVisitor email also sends preregistration emails to your Visitors.

You can add a descriptive display name in addition to the email address. For example, you can create an account called visitors@domain.com with the display name **CertiPath's Visitor Management System**. When your users add visitors@domain.com to their invites, your Visitors will see **CertiPath's Visitor Management System** in the FROM: field of the email.

There are two supported options for using mail with TrustVisitor: IMAP/SMTP and Microsoft Exchange Online (Office 365).

IMAP/SMTP

You can access both Microsoft Exchange Server and Microsoft Exchange Online (Office 365) via the industry standard protocols of IMAP and SMTP. You will need to provide the following details during TrustVisitor mail configuration:

- IMAP and SMTP Servers and Ports
- Whether to use SSL/TLS to connect to the servers
- Username and password for both servers
- The email address and display name

Microsoft Exchange Online (Office 365) via the Graph API

TrustVisitor supports use of the Graph API for mail, but the Exchange Online administrator must configure the following to connect to the Graph API:

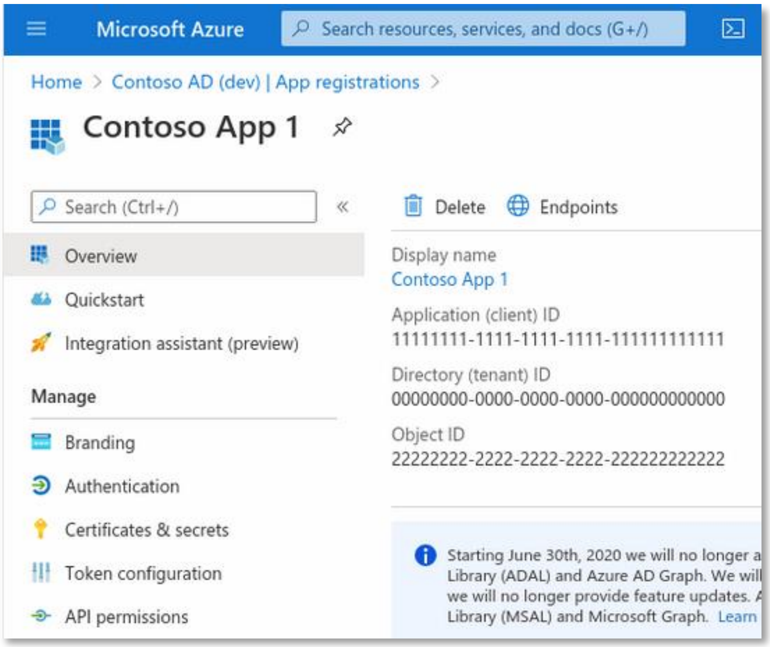
- The Mailbox Login - Normal user mailbox with no special permissions
- The Application (client) ID
- The Directory (tenant) ID

- Either a ClientSecret or a Certificate Thumbprint

To get the last three values, your Exchange Online Administrator needs to access the Azure portal and register an application. The following steps are a TrustVisitor-specific complement to Microsoft's instructions.

1. Log in to https://portal.azure.com.
2. Select **Manage Azure Active Directory**.
3. Select **Manage** > **App Registration** > **New Registration**.
4. Enter a **Name** for the new app registration (e.g., TrustVisitor).
5. Select the appropriate sign-in audience (usually single-tenant).
6. Do not enter a **Redirect URI**.
7. Select **Register**.

   The **App registrations** page appears.



Display name
Contoso App 1

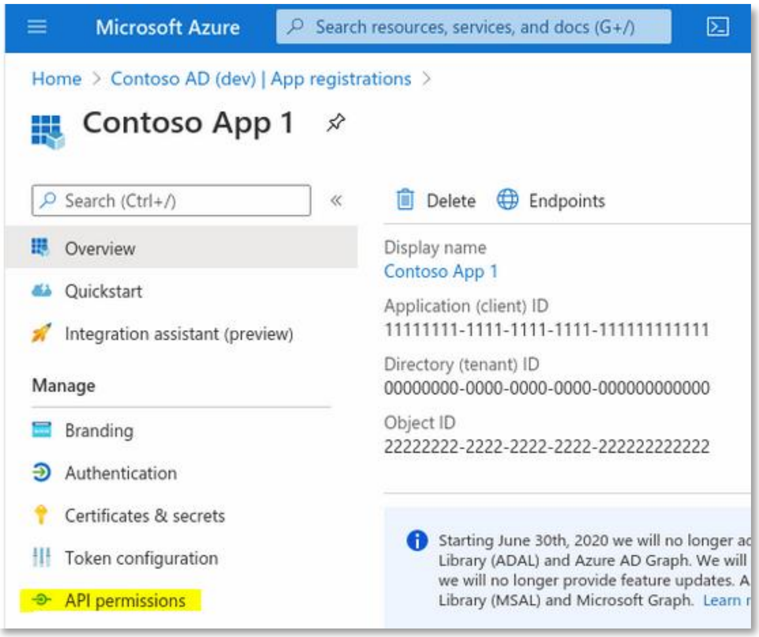
Application (client) ID
11111111-1111-1111-1111-111111111111

Directory (tenant) ID
00000000-0000-0000-0000-000000000000

Object ID
22222222-2222-2222-2222-222222222222

Starting June 30th, 2020 we will no longer a
Library (ADAL) and Azure AD Graph. We will
we will no longer provide feature updates. A
Library (MSAL) and Microsoft Graph. Learn

8. Note the **ClientID** and **TenantID**; you will need them to configure TrustVisitor.
9. Skip **Add a redirect URI**.
10. Proceed with **Add Credentials**. You can add a certificate or client secret. TrustVisitor supports both.
    - If you add a client secret, record the value because you'll need to provide it to TrustVisitor during configuration and it will not appear in Azure again
    - If you're uploading a certificate, make sure you record the certificate thumbprint because you'll need to provide it to TrustVisitor during configuration
11. Configure the permissions required by TrustVisitor.
    a. Navigate back to the **App registrations** page and select **API Permissions**.



Contoso App 1

Display name
Contoso App 1

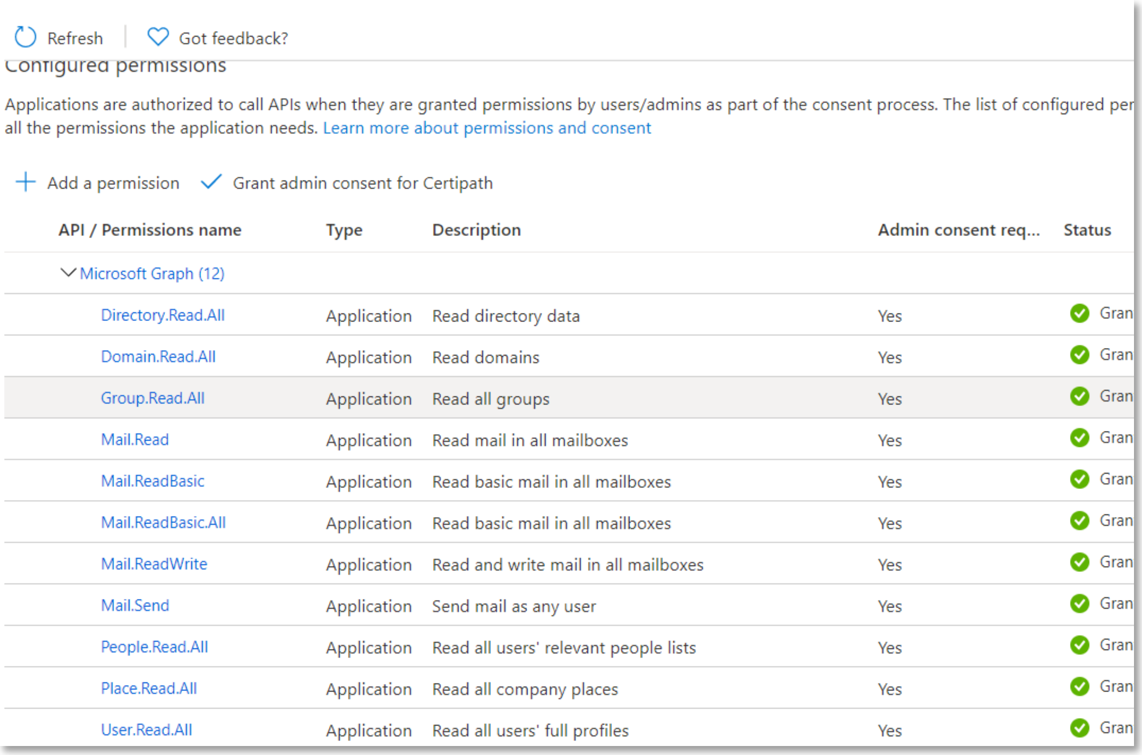
Application (client) ID
11111111-1111-1111-1111-111111111111

Directory (tenant) ID
00000000-0000-0000-0000-000000000000

Object ID
22222222-2222-2222-2222-222222222222

Starting June 30th, 2020 we will no longer ac
Library (ADAL) and Azure AD Graph. We will
we will no longer provide feature updates. A
Library (MSAL) and Microsoft Graph. Learn r

b. Assign the following permissions to the application:



Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured per
all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (12)				
Directory.Read.All	Application	Read directory data	Yes	✓ Gran
Domain.Read.All	Application	Read domains	Yes	✓ Gran
Group.Read.All	Application	Read all groups	Yes	✓ Gran
Mail.Read	Application	Read mail in all mailboxes	Yes	✓ Gran
Mail.ReadBasic	Application	Read basic mail in all mailboxes	Yes	✓ Gran
Mail.ReadBasic.All	Application	Read basic mail in all mailboxes	Yes	✓ Gran
Mail.ReadWrite	Application	Read and write mail in all mailboxes	Yes	✓ Gran
Mail.Send	Application	Send mail as any user	Yes	✓ Gran
People.Read.All	Application	Read all users' relevant people lists	Yes	✓ Gran
Place.Read.All	Application	Read all company places	Yes	✓ Gran
User.Read.All	Application	Read all users' full profiles	Yes	✓ Gran

The **Communication Service** mailbox should be hosted in Exchange (either on-prem, hosted at a provider, or O365).

If using **IMAP/SMTP** to connect, the Communication Service mailbox must be configured to receive meeting invitations as **iCalendar** attachments.

For **Outlook.com** mailboxes this can be found under: Settings->All Outlook Settings->Mail->Sync email->IMAP options->Send event invitations in iCalendar format (ensure it's checked).

Network Requirements

The following network ports and protocols are required by TrustVisitor.

Service/Purpose	Server	Service IP	Protocol	Port	Client
W32Time	Domain Controllers	0.0.0.0	UDP	123	Member Servers & Workstations
RPC-EPMAP	Domain Controllers	0.0.0.0	TCP	135	Member Servers & Workstations
Netbios	Domain Controllers	0.0.0.0	UDP	138	Member Servers & Workstations
RPC	Domain Controllers	0.0.0.0	TCP	49152-65535	Member Servers & Workstations
LDAP	Domain Controllers	0.0.0.0	UDP/TCP	389	Member Servers & Workstations
LDAP SSL	Domain Controllers	0.0.0.0	TCP	636	Member Servers & Workstations
LDAP GC	Domain Controllers	0.0.0.0	TCP	3268	Member Servers & Workstations
LDAP GC SSL	Domain Controllers	0.0.0.0	TCP	3269	Member Servers & Workstations
DNS	Domain Controllers	0.0.0.0	UDP/TCP	53	Member Servers & Workstations
RPC DNS	Domain Controllers	0.0.0.0	TCP	135, 49152-65535	Member Servers & Workstations
Kerberos	Domain Controllers	0.0.0.0	UDP/TCP	88	Member Servers & Workstations
SAM LSA	Domain Controllers	0.0.0.0	NP-UDP/NP-TCP	445	Member Servers & Workstations
AD Group Policy	Domain Controllers	0.0.0.0	ICMP	-	Member Servers & Workstations
SQL	SQL Server	0.0.0.0	TCP	1433	Web/App Servers

Service/Purpose	Server	Service IP	Protocol	Port	Client
RPC/DCOM	SQL Server	0.0.0.0	TCP	1024-65535	Web/App Servers
HTTPS	Web/App Servers	0.0.0.0	TCP	443	Internal Workstations
RDP	Web/App Servers	0.0.0.0	TCP	3389	Internal Workstations
Consul API	Web/App Servers	127.0.0.1	TCP	8500	Web/App Servers (local)
TV Lobby UI	Web/App Servers	0.0.0.0	TCP	443	Internal Systems, Lobby Workstation
TV Admin UI	Web/App Servers	0.0.0.0	TCP	444	Internal Systems
Visitor Registration UI	VR Public Server	0.0.0.0	TCP	8433	Public/DMZ
TV API	Web/App Servers	0.0.0.0	TCP	5333	Internal Systems, Lobby Workstation
Registration API	Web/App Servers	0.0.0.0	TCP	8333	Internal Systems, VR Public Server
Message Queue	Web/App Servers	127.0.0.1	TCP	4150	Web/App Servers (local)
Websockets	Client Workstation	127.0.0.1	TCP	4333	Client Workstation (local)
IMAP	Exchange/Mail Server	0.0.0.0	TCP	143/993	Web/App Servers
SMTP	Exchange/Mail Server	0.0.0.0	TCP	25/26/465/587	Web/App Servers
CA CRL	Internal CA Server/CRL Endpoint	0.0.0.0	TCP	80/443	Web/App Servers
Gallagher API	Gallagher PACS Server(s)	0.0.0.0	TCP	8904	Web/App Servers
CCURE API	CCURE PACS Server(s)	0.0.0.0	TCP	443	Web/App Servers

Service/Purpose	Server	Service IP	Protocol	Port	Client
Identiv API	Identiv PACS Server(s)	0.0.0.0	TCP	2025	Web/App Servers
Identiv SQL	Identiv PACS Server(s)	0.0.0.0	TCP	1433	Web/App Servers
Lenel API	Lenel PACS Server(s)	0.0.0.0	TCP	880	Web/App Servers
Lenel SQL	Lenel PACS Server(s)	0.0.0.0	TCP	1433	Web/App Servers

TrustVisitor Account Requirements

TrustVisitor requires the following accounts:

- Local administrator account for TrustVisitor installation.
- A single domain user account provisioned as a local administrator on the TrustVisitor application server (i.e., ”domain/tv-svc”)
    - The single domain user account must be a group member of the ”Windows Authorization Access” (WAA) Domain Group in the domain that you will be reading employee user accounts from.
    - The single domain user account must be given dbowner, dbreader, and dbwriter on the two TrustVisitor databases (default TrustVisitor.database and TrustVisitor.archive).
        - When the installer is run, this account is provided as the service account, and Windows integrated authentication is chosen for the SQL connection.
        - This is preferable to SQL auth, as the SQL connection will use the Windows Service user context for connecting to the database rather than an SQL user/password credential stored in plain text in the connection string.
        - As a final part of installation config, this account will be specified as the identity used by two of the application service pools.
        - After installation and initialization of the database by the background service, dbowner privileges may be safely revoked for general operations.
- Machine account of the TrustVisitor server for the SQL database connection.
- An email account and SMTP credentials (username and password) for TrustVisitor to communicate with Sponsors, Approvers, and Administrators. This is the account Sponsors will invite to meetings that need Visitor processing. You may wish to give this account a descriptive name, such as trustvisitor@domain.com or visitor-management@domain.com.
- A PACS and/or Validation System account as detailed in the PACS and Validation System Requirements section of this guide.

If the TrustVisitor machine account cannot read from the domain (e.g., NTLM not enabled), separate credentials with read access to the domain will be required.

TrustVisitor Receptionist Workstation Requirements

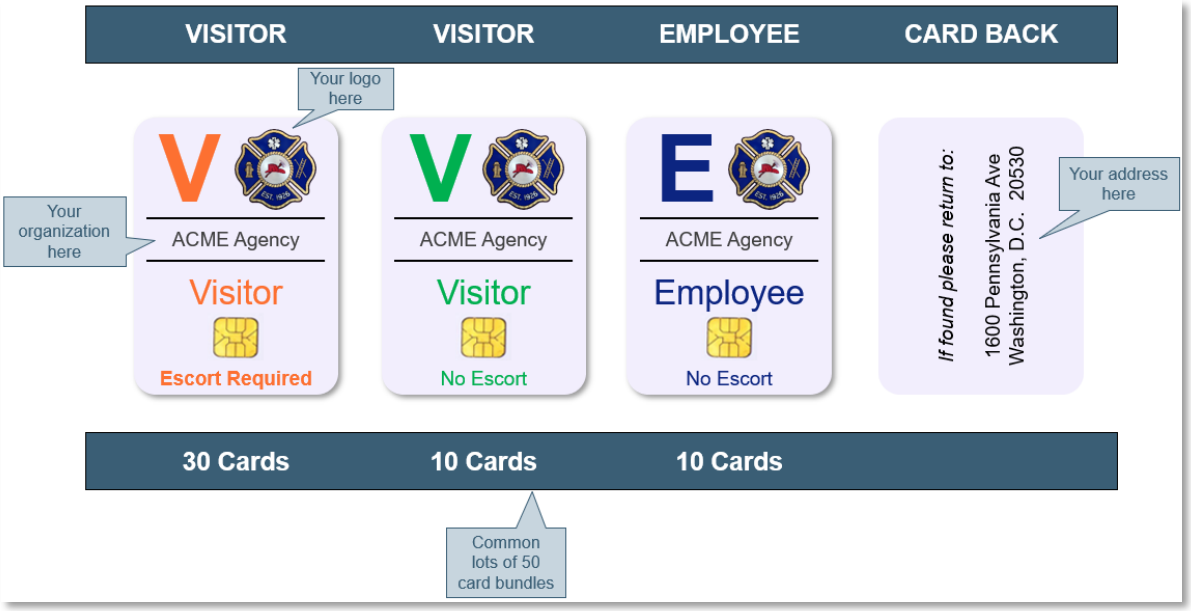
The TrustVisitor workstation that receives Visitors and issues credentials requires a Drivers License Reader, a Smart Card Reader, and a RFID Reader to assign Visitor credentials.

Additionally, WebSockets will need to be installed. WebSockets is a service that runs on the workstation that serves as a local web application. This service enables secures communication between a smart card and the web application and allows registration/assignment of temporary access badges (smart cards) for Employees and Visitors. The web application communicates to the locally running WebSockets server using a host file entry directing the URL to the loop back address. Communication uses a TLS certificate generated at time of installation in the Windows certificate store using the generic hostname for the service.

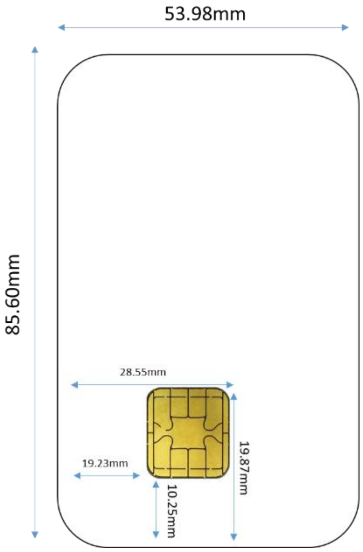
Please review the **TrustVisitor HW and Peripheral Requirements for Lobby Guard Workstation and Kiosk** document for specifics.

Visitor Credential Requirements

The types of Visitor credentials issued by the organization must be defined (e.g., Escort Required, No Escort, Employee, etc.).



You must define the topology of your organization's Visitor credentials (i.e., the card appearance).



- ISO 7810 ID-1 Card Size 85.60 × 53.98 mm
- Printed image is 2024 x 1276 @ 600dpi
- Chip is located:
    - 19.23 mm from left edge
    - 10.25 mm from bottom edge
- Supported topology features:
    - Portrait or landscape
    - Static text and images
    - Dynamic text
    - Color
- Recommendations:
    - While edge-to-edge color is supported, a white background is suggested, with at least 2.5 mm of white space around the borders of the card and contact chip to avoid potential print quality issues.
    - Multiple templates to reflect status (Escort Required, No Escort) and any other relevant scenarios where displaying a name or other information may be a safety concern.
    - The back of the card typically displays terms of use, mustering information, postage guaranteed return address, etc.

PACS and Validation System Requirements

TrustVisitor integrates directly with the organization's PACS. The PACS uses a certificate validation server as part of its operations. TrustVisitor requires access to this system to validate the certificates of Visitor credentials.
Email, Employee ID, or SID is required in the PACS for matching Active Directory users.

The current PACS and Validation Systems supported by TrustVisitor are detailed below:

Type	Brand	API	Additional Requirements
PACS	Lenel OnGuard	OpenAccess	Requires licensing for Partner Integration IPC-309-CRTP01.
PACS	Tyco CCURE 9000	Victor Web Service	Requires licensing for CertiPath - TrustVisitor Web Service Integration - Integration: a35dd48e-fef7-4c69-9ddd-1d6598698fab
PACS	Gallagher PIV Command Centre	Gallagher REST API	
PACS	Identiv Hirsh Velocity	Velocity Sdk	
Validation System	HID pivCLASS	ID Publish	Requires client/server TLS certs for two-way SSL. Working and tested end-to-end integration with PACS is assumed prior to TrustVisitor installation.
Validation System	Innometriks	Innometriks REST API	Requires valid, TLS server certificate installed on ID Server. Working and tested end-to-end integration with PACS is assumed prior to TrustVisitor installation.

OnGuard – PACS

Note: Consult Lenel’s documentation to confirm license and OnGuard installation requirements.

Licensing

The following licenses may be required from Lenel for using TrustVisitor with OnGuard in a FICAM compliant configuration:

- OpenAccess license
- FICAM Authentication license
- Embedded Auth license for every 2 readers

An OnGuard internal account must be created for use by TrustVisitor.

Configuration

OnGuard must be configured to support PIV/FIPS 201 credentials and integrate with HID pivCLASS as the Validation System. OnGuard PIV Badge types must be set up for the required scenarios (e.g. Visitor, Visitor – Escort required, Contractor, Contractor – Escort required, VIP, Employee).

Tyco CCURE 9000 – PACS

Note: Consult Tyco's documentation to confirm license and CCURE 9000 installation requirements.

Licensing

The following licenses must be required from Tyco for using TrustVisitor with CCURE 9000 and Innometriks in a FICAM compliant configuration:

- CCURE 9000 Client
- Victor Web Service API
- CertiPath TrustVisitor API
- Innometriks High Availability

The Victor Web Service API for End-Users requires a feature license in CCURE 9000 and victor products. The Web Service does not allow a connection if the Web Service feature is not licensed on the victor Application Server to which it is trying to connect. Attempting to connect without a license will be rejected with an IIS error message.

Configuration

- CCURE 9000 will require a TLS certificate for the Victor Web Service on the CCURE server.
- A CCURE Operator account for Victor Web Service must be created for use by TrustVisitor.
  - Victor Web Service API on MAS has TLS certificate bound to service that has matching FQDN in Subject Alt Name for the CCURE host.
- CCURE and Innometriks setup for HA support for FIPS-201 credentials, including both PIV and PIV-I card / CHUID formats, as defined by the Innometriks high assurance installation guide.
- Victor Web Service API installed and licensed on MAS
- Licensed CCURE integration on MAS: CertiPath - TrustVisitor Web Service Integration - Integration : a35dd48e-fef7-4c69-9ddd-1d6598698fab
- CCURE has service user account for TrustVisitor defined as an operator with SYSTEM ALL privileges on MAS
- Operator account has requisite database privileges as defined in CCURE documentation
- Innometriks ID Server has TLS certificate bound to web service that has matching FQDN in Subject Alt Name for the IDServer host.
- Innometriks ID Server has a REST operator account defined for TrustVisitor.

Gallagher PIV Command Centre – PACS

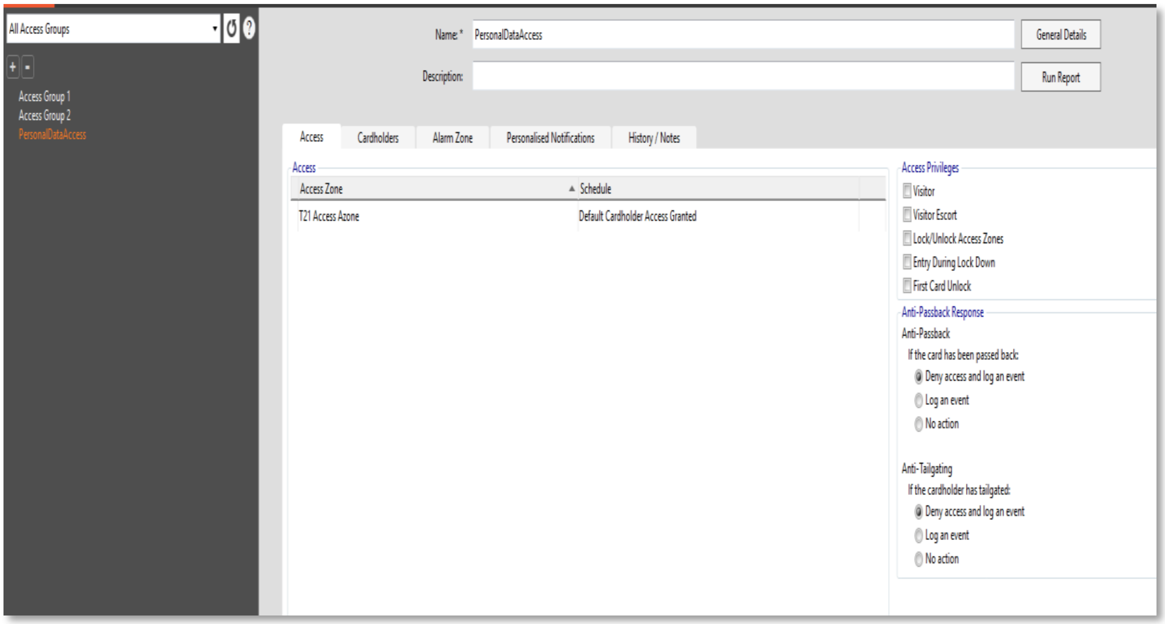
Note: Consult Gallagher's documentation to confirm license requirements.

Licensing

- Obtain API Key for Gallagher system.
- Obtain ssl client certificate for Gallagher system.

Configuration

1. Add the *personaldata* access group.



Access Group 1
Access Group 2
PersonalDataAccess

Name: * PersonalDataAccess
Description:

Access

Access Zone	Schedule
T21 Access Azone	Default Cardholder Access Granted

Access Privileges

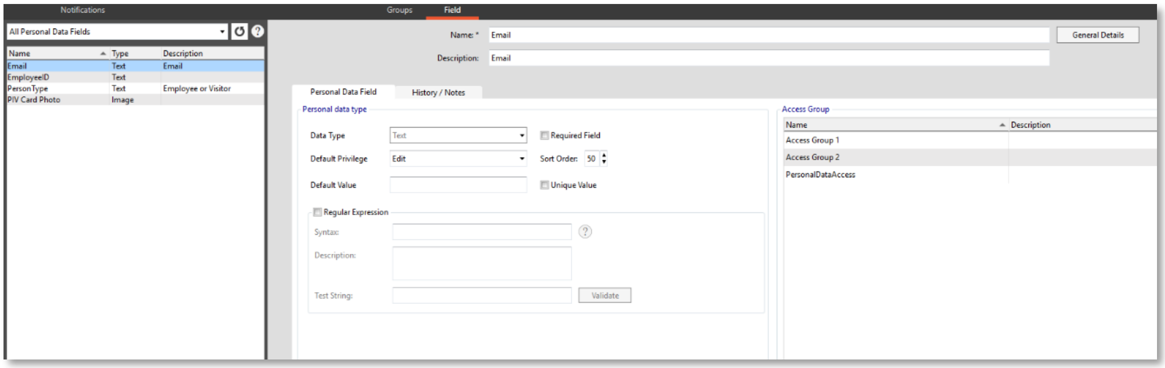
□ Visitor
□ Visitor Escort
□ Lock/Unlock Access Zones
□ Entry During Lock Down
□ First Card Unlock

Anti-Passback Response

Anti-Passback
If the card has been passed back:
● Deny access and log an event
○ Log an event
○ No action

Anti-Tailgating
If the cardholder has tailgated:
● Deny access and log an event
○ Log an event
○ No action

2. Enter an **Email**, **PersonType**, and **Employee ID**.



Name	Type	Description
Email	Text	Email
EmployeeID	Text	
PersonType	Text	Employee or Visitor
PIV Card Photo	Image	

Name: * Email
Description: Email

Personal data type

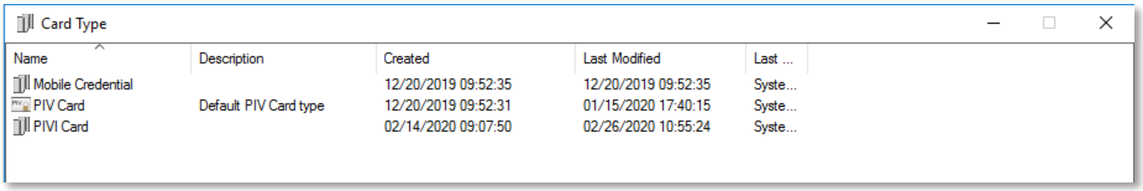
Data Type: Text
□ Required Field
Default Privilege: Edit
Sort Order: 50
Default Value:
□ Unique Value

□ Regular Expression
Syntax:
Description:
Test String:

Access Group

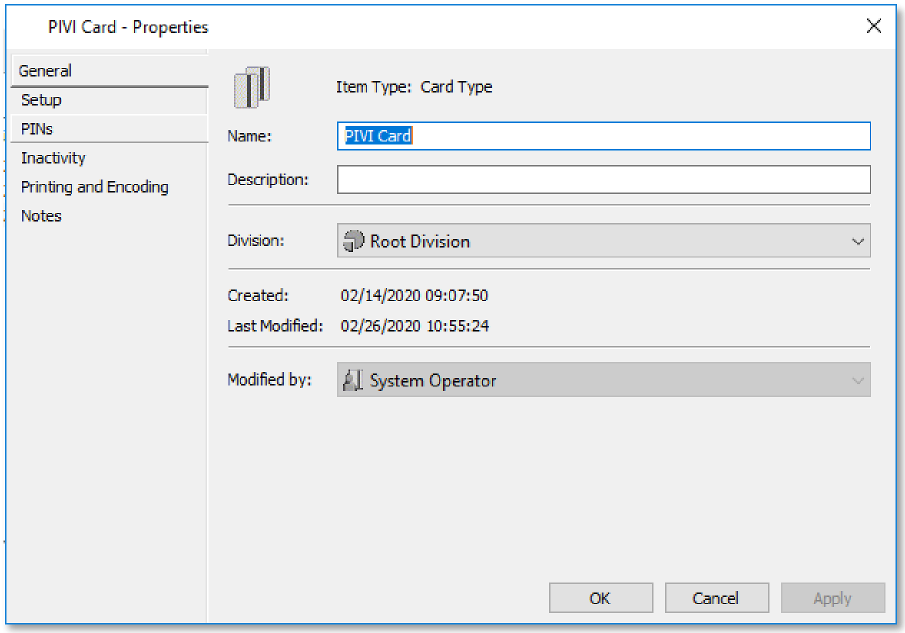
Name	Description
Access Group 1	
Access Group 2	
PersonalDataAccess	

3. Add card types for PIV-I support. PIV Card support is built in already:



Card Type

Name	Description	Created	Last Modified	Last ...
Mobile Credential		12/20/2019 09:52:35	12/20/2019 09:52:35	Syste...
PIV Card	Default PIV Card type	12/20/2019 09:52:31	01/15/2020 17:40:15	Syste...
PIVI Card		02/14/2020 09:07:50	02/26/2020 10:55:24	Syste...



PIVI Card - Properties

Item Type: Card Type

Name: PIVI Card

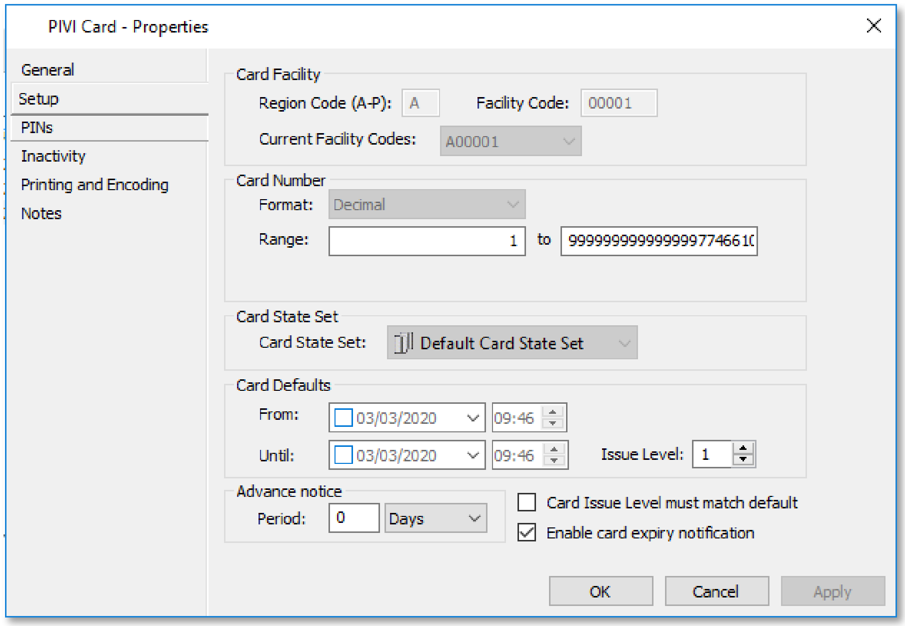
Description:

Division: Root Division

Created: 02/14/2020 09:07:50

Last Modified: 02/26/2020 10:55:24

Modified by: System Operator



PIVI Card - Properties

Card Facility

Region Code (A-P): A Facility Code: 00001

Current Facility Codes: A00001

Card Number

Format: Decimal

Range: 1 to 9999999999999997746610

Card State Set

Card State Set: Default Card State Set

Card Defaults

From: □ 03/03/2020 09:46

Until: □ 03/03/2020 09:46 Issue Level: 1

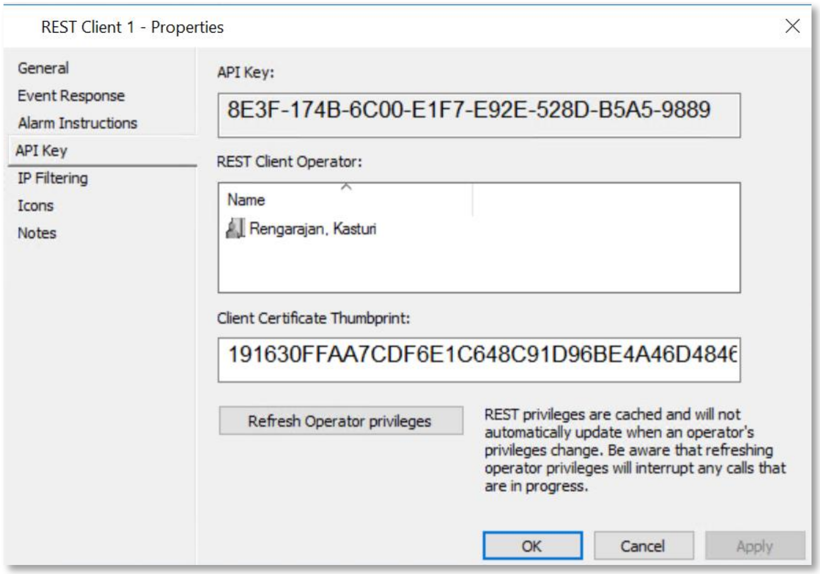
Advance notice

Period: 0 Days

□ Card Issue Level must match default

☑ Enable card expiry notification

4. Create a new REST API Client “service” and assign an operator account.



API Key: 8E3F-174B-6C00-E1F7-E92E-528D-B5A5-9889

REST Client Operator:

Name
Rengarajan, Kasturi

Client Certificate Thumbprint: 191630FFAA7CDF6E1C648C91D96BE4A46D484

REST privileges are cached and will not automatically update when an operator's privileges change. Be aware that refreshing operator privileges will interrupt any calls that are in progress.

Identiv Hirsch Velocity – PACS

HIRSCH by IDENTIV

Licensing

- Install Velocity SDK on the web server.
- Obtain license for the velocity sdk. Instructions are in Identiv Global Services Velocity SDK Developers Guide.

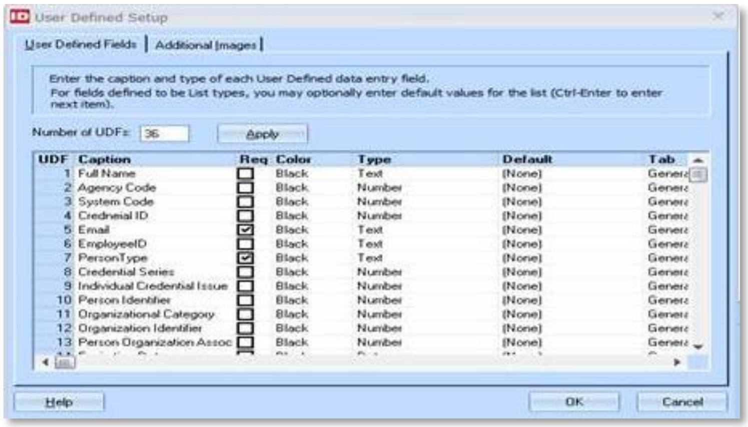
Configuration

Prerequisites

- Velocity Certificate Check Service is installed and configured as per Identiv's specifications.
- Access control is configured appropriately for the templates being used for the solutions.

Steps

1. Enter an employeeid, email, and persontype.

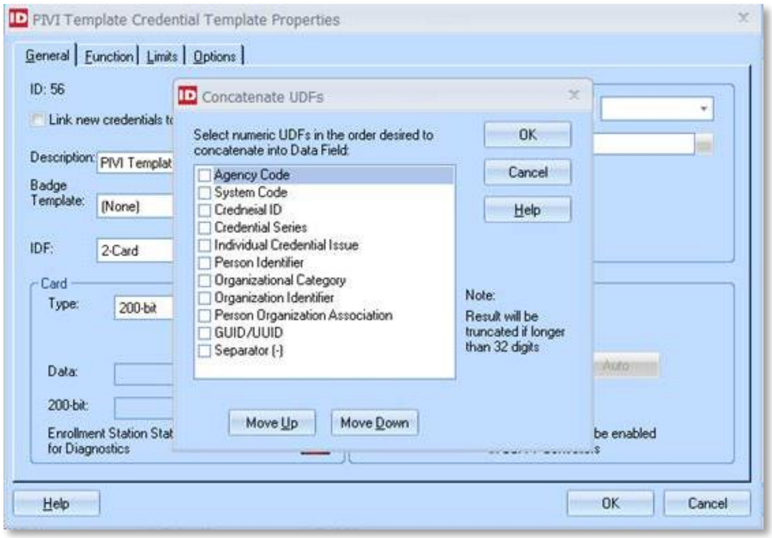


Enter the caption and type of each User Defined data entry field.
For fields defined to be List types, you may optionally enter default values for the list (Ctrl-Enter to enter next item).

Number of UDFs: 36

UDF	Caption	Req	Color	Type	Default	Tab
1	Full Name	□	Black	Text	(None)	Genera
2	Agency Code	□	Black	Number	(None)	Genera
3	System Code	□	Black	Number	(None)	Genera
4	Credneial ID	□	Black	Number	(None)	Genera
5	Email	☑	Black	Text	(None)	Genera
6	EmployeeID	□	Black	Text	(None)	Genera
7	PersonType	☑	Black	Text	(None)	Genera
8	Credential Series	□	Black	Number	(None)	Genera
9	Individual Credential Issue	□	Black	Number	(None)	Genera
10	Person Identifier	□	Black	Number	(None)	Genera
11	Organizational Category	□	Black	Number	(None)	Genera
12	Organization Identifier	□	Black	Number	(None)	Genera
13	Person Organization Assoc	□	Black	Number	(None)	Genera

2. Add credential templates for PIV, PIVI, and Prox. UDF should be turned off since this is for TV only.



PIVI Template Credential Template Properties

General | Function | Limits | Options

ID: 56

□ Link new credentials to

Description: PIVI Templat

Badge Template: (None)

IDF: 2-Card

Card

Type: 200-bit

Data:

200-bit:

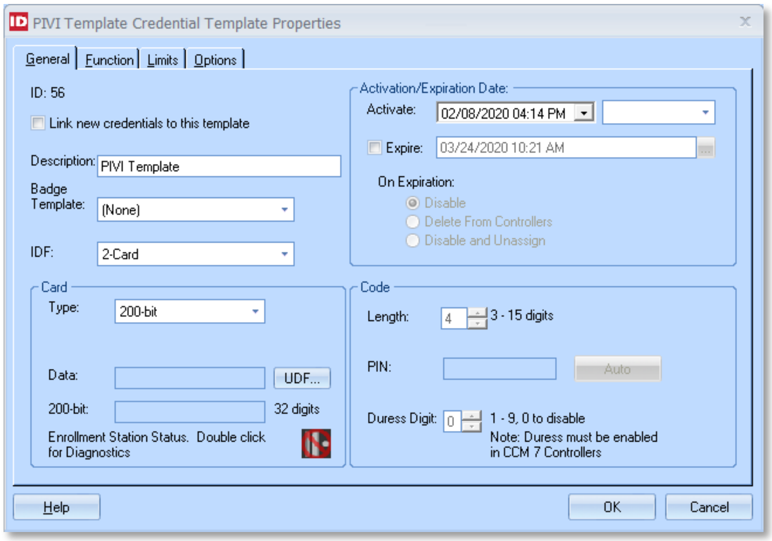
Enrollment Station Stat for Diagnostics

Concatenate UDFs

Select numeric UDFs in the order desired to concatenate into Data Field:

- □ Agency Code
- □ System Code
- □ Credneial ID
- □ Credential Series
- □ Individual Credential Issue
- □ Person Identifier
- □ Organizational Category
- □ Organization Identifier
- □ Person Organization Association
- □ GUID/UUID
- □ Separator (-)

Note: Result will be truncated if longer than 32 digits



PIVI Template Credential Template Properties

General | Function | Limits | Options

ID: 56

□ Link new credentials to this template

Description: PIVI Template

Badge Template: (None)

IDF: 2-Card

Activation/Expiration Date:

Activate: 02/08/2020 04:14 PM

□ Expire: 03/24/2020 10:21 AM

On Expiration:

- ● Disable
- ○ Delete From Controllers
- ○ Disable and Unassign

Card

Type: 200-bit

Data: UDF...

200-bit: 32 digits

Enrollment Station Status. Double click for Diagnostics

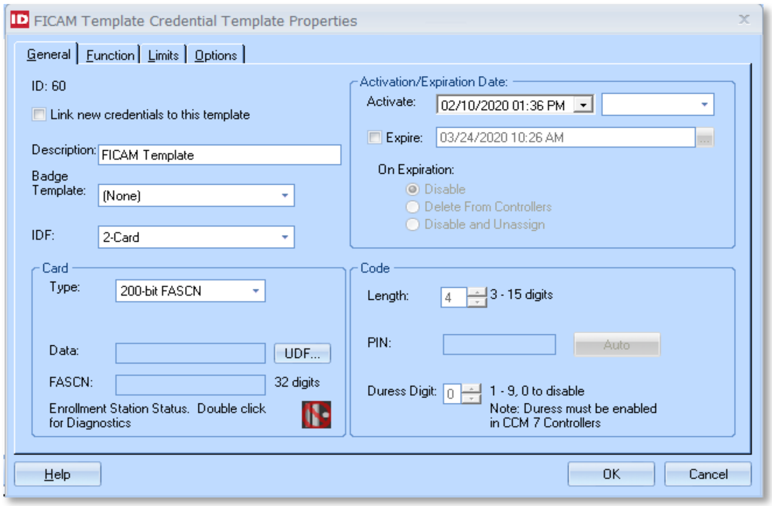
Code

Length: 4 3 - 15 digits

PIN: Auto

Duress Digit: 0 1 - 9, 0 to disable

Note: Duress must be enabled in CCM 7 Controllers



FICAM Template Credential Template Properties

ID: 60

□ Link new credentials to this template

Description: FICAM Template

Badge Template: (None)

IDF: 2-Card

Activation/Expiration Date:

Activate: 02/10/2020 01:36 PM

□ Expire: 03/24/2020 10:26 AM

On Expiration:
● Disable
○ Delete From Controllers
○ Disable and Unassign

Card

Type: 200-bit FASCN

Data:

FASCN: 32 digits

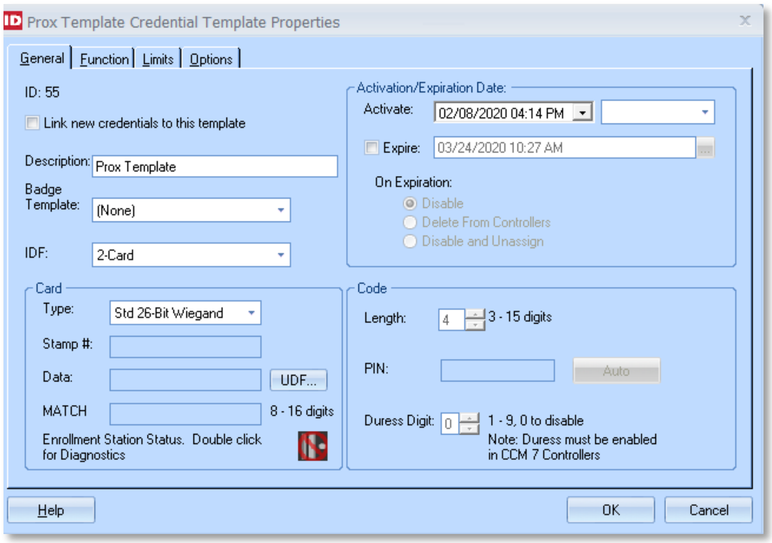
Enrollment Station Status. Double click for Diagnostics

Code

Length: 4 3 - 15 digits

PIN:

Duress Digit: 0 1 - 9, 0 to disable
Note: Duress must be enabled in CCM 7 Controllers



Prox Template Credential Template Properties

ID: 55

□ Link new credentials to this template

Description: Prox Template

Badge Template: (None)

IDF: 2-Card

Activation/Expiration Date:

Activate: 02/08/2020 04:14 PM

□ Expire: 03/24/2020 10:27 AM

On Expiration:
● Disable
○ Delete From Controllers
○ Disable and Unassign

Card

Type: Std 26-Bit Wiegand

Stamp #:

Data:

MATCH 8 - 16 digits

Enrollment Station Status. Double click for Diagnostics

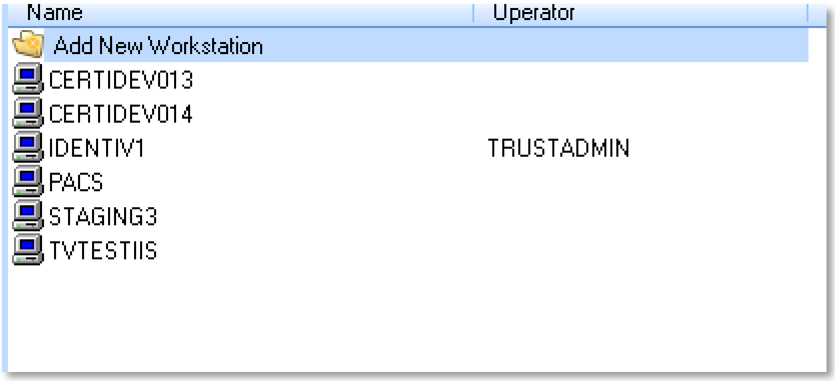
Code

Length: 4 3 - 15 digits

PIN:

Duress Digit: 0 1 - 9, 0 to disable
Note: Duress must be enabled in CCM 7 Controllers

3. Add the workstation where Velocity SDK is installed.



Name	Operator
Add New Workstation	
CERTIDEV013	
CERTIDEV014	
IDENTIV1	TRUSTADMIN
PACS	
STAGING3	
TVTESTIIS	

HID pivCLASS – Validation System

Note: Consult HID’s documentation to confirm license requirements.

You may need an IDPublisher license for HID pivCLASS to integrate with TrustVisitor.

HID pivCLASS requires a TLS certificate for the IDPublish website on the HID pivCLASS server.

Innometriks – Validation System

Innometriks requires a TLS certificate for the Innometriks REST website on the CCURE server.

A REST user account must be created for use by TrustVisitor.

Addendum

Important Changes as of TrustVisitor v4.0:

TrustVisitor Azure AD API Least Privilege Configuration

Note: Replace [APPID-GUID] and [MAILBOX-USER] with client-specific strings during configuration.

I. Create [MAILBOX-USER] Office 365 account with email and calendar permissions, as described in the TrustVisitor installation requirements.

II. Disable login for the [MAILBOX-USER] account in Office 365 / Microsoft Entra:

1. In Azure Active Directory, uncheck “User Login Enabled” for the [MAILBOX-USER] account.
2. Confirm that the selected O365 mailbox user status shows as “Login Blocked”.

III. Create and configure “TrustVisitor” Enterprise Application in Azure AD:

1. Confirm Tenant ID and provide to the TrustVisitor installation team.
2. Confirm Application ID (aka Client ID) and provide to the TrustVisitor installation team.
3. Add [MAILBOX-USER] as Enterprise Application User

IV. Configure “TrustVisitor” Application Registration in Azure AD:

1. Establish API Key Secret and securely convey to the TrustVisitor installation team.
2. Set API Privileges – Microsoft Graph API, Application:
   - *Mail.ReadWrite*
   - *Mail.Send*
   - *Place.Read.All*
3. Grant Admin Consent for the API privileges listed above.

V. Execute PowerShell script to restrict API privileges to the specified [MAILBOX-USER] O365 account:

1. Access Office 365 Exchange PowerShell as an administrator.

   connect-ExchangeOnline -UserPrincipalName [ADMIN-UPN@DOMAIN.COM]

2. Run the following script in PowerShell:

- *New-ApplicationAccessPolicy -AppId [APPID-GUID] -PolicyScopeGroupId [MAILBOX-USER] -AccessRight RestrictAccess -Description "Restrict TrustVisitor Application ID API Privilege to [MAILBOX-USER]."*

Confirm that PowerShell executes successfully.

3. Run the following script in PowerShell to validate that the selected mailbox is accessible to the API scope:

   Test-ApplicationAccessPolicy -Identity [MAILBOX-USER] -AppId [APPID-GUID]

   Confirm PowerShell executes successfully and returns an “AccessCheckResult: Granted” status.

4. Run the following script in PowerShell to validate that other mailbox accounts are not accessible to the API scope:

   Test-ApplicationAccessPolicy -Identity [ANY-OTHER-MAILBOX-USER] -AppId [APPID-GUID]

   Confirm PowerShell executes successfully and returns an “AccessCheckResult: Denied” status.