300 Horizon Dr. Suite 308 Hamilton, NJ 08691
+(609) 270-3220
info@princetonidentity.com
www.princetonidentity.com

Pre-Installation Requirements and Preparation

This document covers information necessary for a smooth and efficient installation of your new EyeAllow and/or Access200w edge device(s) along with the required IDS software. *Please note that some of these items may have a non-trivial lead time* based on external factors (eg API licenses from your access control system provider) and internal factors (eg port and IT security settings, requiring availability by your internal IT team), so please plan accordingly to ensure that 'installation day' is free from unexpected delays.

Preparation and requirements necessary for installation will be reviewed through these five steps:

Step 1 – Prepare your IT environment

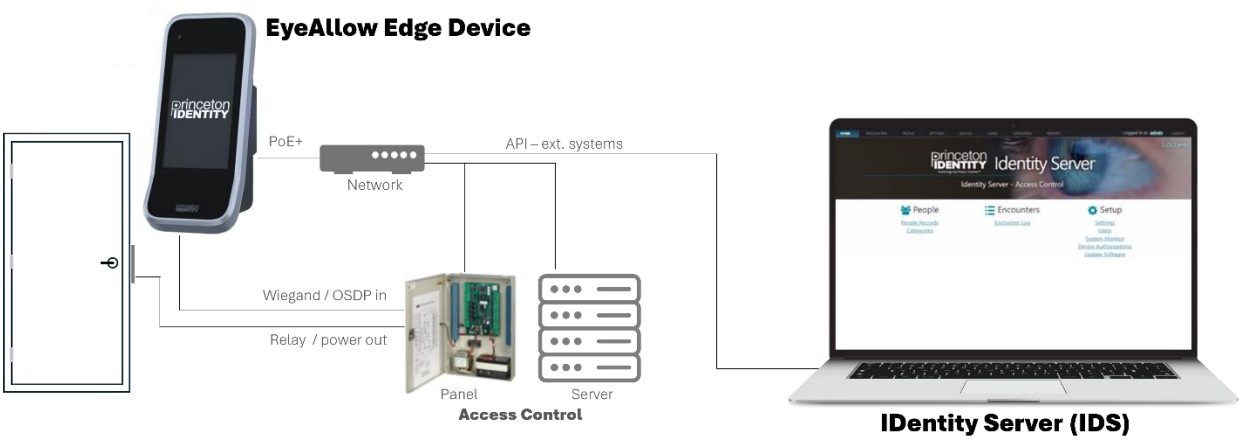
Step 2 – Prepare to install the IDS software

Step 3 – Prepare to sync IDS with your Access Control

Step 4 – Prepare for physical installation of edge devices

Step 5 – Prepare system for use

We recommend that you read through this entire document to familiarize yourself with the complete process before proceeding to step 1. Full installation instructions are linked at the end of each section.



300 Horizon Dr. Suite 308 Hamilton, NJ 08691
+(609) 270-3220
info@princetonidentity.com
www.princetonidentity.com

Check List of Pre-Installation activities

- ☐ Network ports and traffic properly configured [step 1]
- ☐ IP addresses unconflicted [step 1]
- ☐ IDS server installed and meeting system requirements; separate but connect-able to access control server [steps 1, 2]
- ☐ Hardware acceleration settings confirmed [step 2]
- ☐ Ensure all credentials are in place (access control, LDAP, etc.) [steps 2, 3]
- ☐ Access Control system API license acquired - if needed [step 3]
- ☐ Device location considered, all wiring specs met [step 4]
- ☐ PoE+ power available, and power sourcing equipment is properly configured [step 4]

300 Horizon Dr. Suite 308 Hamilton, NJ 08691
+(609) 270-3220
info@princetonidentity.com
www.princetonidentity.com

Step 1 – Prepare your IT network environment

Princeton Identity's Identity Server and Edge Devices assumes that certain ports and network configurations are made available for proper functionality. Please refer to the information below and make sure that the following network configurations are properly established.

- Ensure that the following ports are open or configured in the system's firewall to allow IDS and the devices to communicate. If separate VLANs are used, please confirm that traffic between the server/s and edge devices can communicate between VLANS:
    - **Service Name:** PI Identity Server
      Protocol/Port(s): HTTPS/8443, HTTP/80 (redirects to 8443)
    - **Service Name:** postgresql
      Protocol/Port(s): TCP/5432 (internal)
    - **Service Name:** sql server (only if using Microsoft SQLServer instead of PostgreSQL)
      Protocol/Port(s): TCP/1433 (internal)
    - **Protocol/Port:** 587
      Purpose: SMTP if enabled
    - **Edge devices (including EyeAllow and Access200w):**
      Inbound TCP – HTTPS/443
      Inbound TCP – HTTP/80 (redirects to 443)
- If a PACS, time & attendance, or any other integration is used (step 3), confirm that the necessary ports and IP addresses are configured on the firewall and IDS's host OS to allow traffic between the integration's services and IDS.
- Setup a server or virtual machine running Windows (see table below) for IDS installation. We recommend that IDS should be the only application running on the server / VM.
- The IDS uses the system's IPv4 address by default. This address cannot be used simultaneously with another application/program/device on the 8443 port.
- If configuring edge devices with a static IP address, verify that the DHCP server has not assigned that address prior to configuring the device's IP address.
- If installing IDS on a Laptop or desktop for a proof of concept, please remove all external docks and network adaptors (dongles) during the licensing steps. If the external networking adaptors are not removed the license will be attached to the adaptor instead of the IDS.

Once you have worked through the pre-installation activities above, please proceed to step 2 below to follow the preparations and requirements necessary for installing the IDS software.

300 Horizon Dr. Suite 308 Hamilton, NJ 08691
+(609) 270-3220
info@princetonidentity.com
www.princetonidentity.com

Step 2 – Prepare to install the IDS software

PI's identity assurance solution consists of two main components: Identity Server (IDS) and edge devices (EyeAllow and/or Access200w). Identity Server can be installed on either a dedicated server or a virtual machine; please ensure the following minimum requirements are met:

Requirement	IDS Install Type	Specification
Operating System	Windows (x64)	Windows Server 2016, 2019, 2022, 2025, & Windows 10, 11
Processor	Windows (x64)	For Intel: Haswell (2013) and newer (not including Pentiums or Celerons) For AMD: Excavator (2015) and newer
Storage	Windows (x64)	256 GB

Below are the additional Identity Server configuration options that we offer:

Item	Description	Details
LDAP	Microsoft Active Directory / Entra	Windows Server 2016, 2019, 2022, 2025, & Windows 10, 11
Virtualization	*Microsoft Hyper-V VMware vSphere (ESXi) 6.7 Oracle VM VirtualBox 6.1	*Hosted on Windows 10, Windows Server 2016, 2019, 2022, & 2025
Database	Microsoft SQL Server 2017, 2019, & 2022	See article 6.1. Connecting Identity Server to Microsoft SQL Server
Database	PostgreSQL 10, 11, 17	

300 Horizon Dr. Suite 308 Hamilton, NJ 08691
+(609) 270-3220
info@princetonidentity.com
www.princetonidentity.com

To achieve minimum matching performance (under 1 second), PI recommends the following specifications based on user base size and number of devices (with assumptions made to account for typical use frequency):

Enrollees per IDS	1,000	10,000	100,000	300,000
Edge Device per IDS	20	75	150	300
Cores	4	8	8	16
Memory	8GB	8GB	16GB	32GB

The following additional items should also be noted prior to installing PI's IDS:

- PI's IDS will only support the listed operating systems at this time. Using a non-specified OS will cause issues.
- IDS SHOULD NOT be installed on the same server that is running your current access control system, or on any preconfigured access control appliance. This will cause issues.
- The face matcher within the Identity Server requires FMA3 instructions (for hardware acceleration). You can verify your server is equipped with this hardware acceleration feature by running Microsoft's Coreinfo program. Follow these steps:
    - Extract the contents of Coreinfo.zip (from Microsoft) to a folder (Local Disk [C:] > generally System32 or System64)
    - Run Coreinfo or Coreinfo64.exe from a command prompt
    - If this hardware acceleration feature is enabled, the following line should appear in the output list: "FMA * Supports FMA extensions using YMM state"
    - Note that the "*" character is critical because it means that hardware acceleration feature is enabled/available.
    - If FMA3 is not enabled, the installer may work but IDS may not start up

You will also need to ensure that integration with an external service that uses a custom Certificate Authority is enabled, as IDS supports integrations with several external services. For example...

- Synchronizing access controls credentials with an access control server (ex CCURE, OnGuard)
- Authentication with an LDAPS server.

300 Horizon Dr. Suite 308 Hamilton, NJ 08691
+(609) 270-3220
info@princetonidentity.com
www.princetonidentity.com

These services are often configured to require use of a custom Certificate Authority (CA). In order for IDS to properly communicate with these services, the custom CA's public certificate needs to be added to the trust store of the IDS (shown in step 3). This will ensure that IDS trusts the certificates issued by the custom CA.

- First, obtain the Custom CA's Public Certificate. This certificate is usually provided by the administrator of the external service or can sometimes be extracted from the service itself using tools like OpenSSL.
- Export the certificate as a DER binary
- Then copy the certificate to the machine that IDS will be running on

Once you have worked through all of the pre-installation activities in steps 1 and 2 above, please only then follow the installation guide found on Princeton Identity's support site to complete the installation of IDS software on your chosen server: Windows Installation. Note that depending on your security settings, our install and update files may need to be unblocked after downloading, prior to usage. Then proceed to step 3.

300 Horizon Dr. Suite 308 Hamilton, NJ 08691
+(609) 270-3220
info@princetonidentity.com
www.princetonidentity.com

Step 3 – Prepare to sync IDS with your Access Control

Princeton Identity's IDS natively supports 3rd-party integrations to allow for synchronizing and interacting with Access Control, Point of Sale, Time and Attendance, etc. systems. This process eliminates manual data entry and associated human error and speeds up the onboarding process. Alternatively, user/profile data sync can also be imported and synchronized via a .csv, .xls, or .xlsx file import.

As stated in step 2, in order for IDS to properly communicate with your access control server, the custom CA's public certificate needs to be added to the trust store of the IDS. That is, you need to import the certificate into the Java KeyStore used by IDS.

- Open a terminal on the IDS machine with Administrative privileges
- Navigate to the folder containing the certificate (ex filename: certificate.der)
- Run the following command (replace certificate.der with the name of the actual certificate file)
    - *keytool -importcert -alias identity-client.key -keystore "%JAVA_HOME%\lib\security\cacerts" -storepass changeit -file certificate.der*
- Restart the IDS service

Also, some of these API integrations will require a license from the manufacturer to specifically enable our IDS to pull data from the access control / etc. system. *Be aware that obtaining this license may take up to 2 weeks (depending on the manufacturer), so please plan accordingly*. In particular, the following popular access control systems require the hosting organization to purchase such a license:

- Genetec
- Honeywell ProWatch
- Lenel OnGuard
- CCure 9000

As noted in step 1, the Identity Server will need to have connectivity to the access control server for any sync to be successful. First confirm this connection is active and then ensure you have any necessary access control manufacturer licenses. Please note the license part numbers are shown in the table below showing a list of all manufacturers / products that are currently supported by PI's IDS. Once you have worked through all of the pre-installation activities above, you can then initiate the sync between IDS and your access control system by following the appropriate instructions linked in the final column of the table below.

300 Horizon Dr. Suite 308 Hamilton, NJ 08691
+(609) 270-3220
info@princetonidentity.com
www.princetonidentity.com

Access Control System	Version(s) PI supports	Manufacturer License Required Specific to PI's API	Princeton Identity's Configuration Guide
Additional Identity Server (Parent/Child configuration)	All	N/A	Deploying Identity Server for High Availability – Princeton Identity
American Direct AccessNSite	7.9.47	No	AccessNSite Integration
Avigilon ACM/Unity	6.50, 7.12	No	Avigilon Unity Integration Setup
Avigilon Alta (formerly OpenPath)	Cloud-based, automatically upgraded	No	Avigilon Alta Integration Setup
AMAG Symmetry	9.12.0	No	AMAG Symmetry Integration Setup
Atrium	Atrium Campus	No	Atrium Campus POS Integration Setup
Brivo Access	Cloud-based, automatically upgraded	No	Brivo Access Integration Setup
Feenics Access Control	v3 previously, now cloud-based / automatically upgraded	No	N/A
Galaxy System Galaxy	10.4.8, 11.3	No	System Galaxy Integration Setup
Gallagher Security Command Centre	8.90, 9.20	No	Gallagher Security Command Center Integration Setup
Genetec Security Center	5.7, 5.9, 5.11, 5.12, 5.13	GSC-1SDK-PRINCETONIDENTITY-ACS (Qty: 2)	Genetec Security Center Integration Setup
Honeywell Pro-Watch	4.3.5 (HSDK 2.5.0), 4.5 (HSDK 2.6.0)	PWHSDK64 or PWHSDK64-R PWHSDK256 or PWHSDK256E for door counts > 64 ...may be needed, contact Honeywell	Pro-Watch Integration Setup
ICT Protégé GX	4.3.352.7	No	ICT Protege GX Integration Setup
Lenel OnGuard	7.3, 7.4, 7.5, 7.6, 8.0, 8.1, 8.2, 8.3	For OnGuard version 7.3, 7.4, 7.5: IPC-091-PRIDEN01 For OnGuard version 7.6, 8.0, 8.1, 8.2. 8.3: IPC-094-PRNID01-B	Lenel OnGuard Integration Setup
Lenel S2 NetBox	4.10, 5.3, 5.4, 5.6	No	Lenel S2 NetBox Integration Setup
Paychex Flex Time	Cloud-based, automatically upgraded	No	Paychex Flex Time Integration Setup
RS2 AccessIT!	9.1.2, 11.2.1	No	RS2 Access It! Integration Setup
CCURE 9000	2.60, 2.70, 2.80, 2.90, 3.0, 3.1	CC9000-IOM for SRI IOM Integration (prior to August 2024), CC9WS-PRINCE (August 2024-on)	C CURE 9000 Integration Setup
Schneider Electric Security Expert	4.3.370.19	No	Schneider Electric Security Expert Integration Setup
TouchNet	Cloud-based, automatically upgraded	No	TouchNet Integration Setup

*Lenel Series 3 boards are the only ones compatible with our solution. Series 2+ may pose functionality issues.

300 Horizon Dr. Suite 308 Hamilton, NJ 08691
+(609) 270-3220
info@princetonidentity.com
www.princetonidentity.com

Step 4 – Prepare for physical installation of edge devices

PI's identity assurance solution consists of two main components: Identity Server (IDS) and edge devices (EyeAllow and/or Access200w). Before installing your edge device(s) as either wall mount / permanent location or on a portable stand / bench-top evaluation, review the following and ensure all requirements are met.

- Consider device location (see the support site article for guidance): Mounting location considerations for outdoor devices
- Use only Cat 5e or higher Ethernet cable from the network switch to all edge device locations
- PI edge devices require Power over Ethernet (PoE+ standard 802.3at Type 2 [30 Watts]) for power
    - Note: ensure that the output of any/all network switches are properly configured to output 30W. Managed switches that are not set to this rating will cause functionality issues with the devices when attempting to conserve power.
    - Some older Cisco switches require these following settings to be enabled: "Power inline port 2-event", "Power inline police", and "Power inline static max: 30000" to ensure that the port will support the full 30W required without negotiation.
    - If the PoE+ switch is configured for Allocation-by-Class, it is likely that LLDP will need to be disabled for the applicable port. Neither the EyeAllow nor Access200w utilize LLDP and certain switches are known to negotiate improperly when the reader first boots with those settings. Disabling LLDP or using Allocation-by-Value (30W) will result in normal behavior.
- The EyeAllow & Access200w are set to DHCP by default. When a DHCP server is not available, the device will fallback to Automatic Private IP Addressing (APIPA) in the range of 169.254.0.0/16. This IP address will be assigned automatically until a DHCP server is found or a static IP is set. The device's network setting can be configured on the device's display by going to Setting > Network.
- If you are connecting your edge device to the access control panel, use Wiegand wires or RS-485 (if using OSDP) from the access control panel to all edge device locations.

If your final identity assurance system will be able to read RF cards or digital mobile credentials – requiring a card reader either internal to the edge device or external to the edge device – then you will first need understand the card format, data structure, and any potential encryption deployed and then ensure that the IDS and edge device SW is properly configured.

For reference, PI internal card readers – when properly configured – are capable of reading the card types and formats shown in the table below.

300 Horizon Dr. Suite 308 Hamilton, NJ 08691
+(609) 270-3220
info@princetonidentity.com
www.princetonidentity.com

Item	Type	Comments
Internal Card Reader	Low frequency RFID (125 kHz)	HID Prox, Indala Prox, EM Prox, EM4100/4102/4200/4305/4450, AWID Prox, Hitag 1.2.3, ASK, PSK, FSK
	High frequency RFID (13.56 MHz)	iCLASS, iCLASS SE/SR, iCLASS Seos, MIFARE Classic, MIFARE DESFire 0.6, MIFARE DESFire EV1/EV2, MIFARE Ultralight C, MIFARE Ultralight, FeliCa (Idm) CEPAS (CAN), ISO 14443A/B, ISO15693, Support for ISO18092 NFC Tag type 1, 2, 3, 4, 5, T=CL, SmartMx Contact support@princetonidentity.com for cards using encryption keys.
External Card Readers (Customer-supplied)	Wiegand	Does not include mag stripe readers, card readers with built-in PIN pads, or external readers via OSDP connection.

Certain cards such as MIFARE Classic/DESFire/Plus, and HID iClass Elite require keys and memory information to be configured on the internal reader to read PACS data. HID credentials can be loaded using existing HID key loading cards you may have in your possession. For other card inquiries that utilize encryption, please contact support so the appropriate configuration can integrated into your internal card reader.

Once you have worked through all of the pre-installation activities above, please follow the installation guide found on Princeton Identity's support site to complete the installation of edge device(s): Device Installation and Wiring, cont'd. Note that once installation is complete, we recommend that each edge device should undergo a short proximity sensor calibration, as device calibration is dependent on installation environment. The calibration guide can be found on Princeton Identity's support site: Proximity Sensor Calibration. Then proceed to step 5.

300 Horizon Dr. Suite 308 Hamilton, NJ 08691
+(609) 270-3220
info@princetonidentity.com
www.princetonidentity.com

Step 5 – Prepare system for use

PI's identity assurance solution consists of two main components: Identity Server (IDS) and edge devices (EyeAllow and/or Access200w). Before using the system, you must first pair / connect the edge devices with your IDS. Detailed instructions for doing so can be found in the Manuals and Guides section of Princeton Identity's Support website (Connecting edge devices to the IDS).

Note that Identity Server and edge devices support username and password authentication of built-in user accounts. Additionally, an Identity Server can be configured to use LDAP (Active Directory) or SSO (SAML) for authentication. Once an edge device has been connected to Identity Server, the edge device's default admin account is disabled. You must use a valid Identity Server user account to login as it inherits it. These include accounts automatically created by the LDAP authentication. If the device becomes disconnected from Identity Server, the default admin account becomes re-enabled.

For convenience, an operator can login to Identity Server and use the Devices tab to access the connected devices. If the user has the admin role permission, the Devices page will generate hyperlinks to click on which will open the device's administration page and will not require login credentials to be reentered.

Instructions for configuring LDAP (Active Directory) authentication in IDS can be found in the Manuals and Guides section of Princeton Identity's Support website (3.18 LDAP User Authentication Configuration – Princeton Identity).

For reference, here is a list of the system's default usernames and passwords.

- **System/Device:** EyeAllow/Access200™ administration web page local admin account
  Username: admin
  Password: password
  Can it be changed?: The username can't be changed, but the password can be changed on the device's web page. This account is disabled when the device is connected to an IDS.
- **System/Device:** Identity Server administration web page
  Username: admin
  Password: password
  Can it be changed?: Both the username and password can be changed on the Identity Server's settings.
- **System/Device:** PostgreSQL
  Username: postgres
  Password: postgres
  Can it be changed?: The username and password can be changed through the operating system.

300 Horizon Dr. Suite 308 Hamilton, NJ 08691
+(609) 270-3220
info@princetonidentity.com
www.princetonidentity.com

The Identity Server has 3 user roles: admin, enroller, and basic. For reference, the description of each user role is shown below.

- **Admin:** An administrative user role with full access which can view, add, and edit all people information, users, and system settings for the IDS application and connected devices.
- **Enroller:** An enrollment operator user role which can view, add, and edit all people information. They can also view encounters and system health for connected devices.
- **Basic:** A read-only user role which can view all people information. They can view encounters and system health for connected devices.

Please feel free to contact us if you have any questions/concerns/inquiries. We can be reached by phone (609-270-3220) or email (support@princetonidentity.com).

300 Horizon Dr. Suite 308 Hamilton, NJ 08691
+(609) 270-3220
info@princetonidentity.com
www.princetonidentity.com

Thank you for choosing Princeton Identity!

For over 20 years, Princeton Identity has developed and manufactured state-of-the-art commercial iris-biometrics for access control, time and attendance, point of sale, and border applications. In proven installations around the world, our customers manage their entire identity lifecycle with our convenient and elegant multi-factor authentication edge devices backed by the proprietary Iris-on-the-Move™ technology and our custom identity server software. Together these components enable a total solution with exceptional flexibility, accuracy, and convenience, and all with future-proof scalability and an unexpectedly low total cost of ownership.

Iris biometrics are THE future of identity assurance in part because the iris is simultaneously the most unique AND the most stable identifying human feature (more than DNA, and WAY MORE than your face). With Princeton Identity's iris-authentication, we deliver touchless and highly spoof-resistant solutions that are unaffected by weather or lighting, and work perfectly well with any amount of head coverings or equipment, protective masks, sunglasses, makeup… whatever.

We see you, not your appearance!

In addition, Princeton Identity products are extremely scalable and flexible, able to manage millions of individuals within a wide variety of system and application requirements. The total solution can be configured for multi-factor authentication by polling any combination of six distinct credential-types: iris, face, mobile digital credential, physical card, pin pad, and QR code scanning… all in one small edge device. As a bolt-on solution, installation is a breeze with single wire power and data connection, and pre-developed API integrations with dozens of the most common security and payment platforms. And because system management is done through a high-UX web-portal, administration is low overhead, and further made easy with seamless enrollment and other efficiency-minded features.

Princeton Identity's world-class iris-biometrics identity solutions offer the pinnacle of accuracy and convenience, and are ideally suited for any campus / corporate operations or critical infrastructure protection. It's no wonder premier global organizations rely on our products!