

802.1X Technology

Safety Instructions

Safety Instructions • English

WARNING: This symbol, , when used on the product, is intended to alert the user of the presence of uninsulated dangerous voltage within the product's enclosure that may present a risk of electric shock.

ATTENTION: This symbol, , when used on the product, is intended to alert the user of important operating and maintenance (servicing) instructions in the literature provided with the equipment.

For information on safety guidelines, regulatory compliances, EMI/EMF compatibility, accessibility, and related topics, see the Extron Safety and Regulatory Compliance Guide, part number 68-290-01, on the Extron website, www.extron.com.

Sicherheitsanweisungen • Deutsch

WARNUNG: Dieses Symbol , auf dem Produkt soll den Benutzer darauf aufmerksam machen, dass im Inneren des Gehäuses dieses Produktes gefährliche Spannungen herrschen, die nicht isoliert sind und die einen elektrischen Schlag verursachen können.

VORSICHT: Dieses Symbol , auf dem Produkt soll dem Benutzer in der im Lieferumfang enthaltenen Dokumentation besonders wichtige Hinweise zur Bedienung und Wartung (Instandhaltung) geben.

Weitere Informationen über die Sicherheitsrichtlinien, Produkthandhabung, EMI/EMF-Kompatibilität, Zugänglichkeit und verwandte Themen finden Sie in den Extron-Richtlinien für Sicherheit und Handhabung (Artikelnummer 68-290-01) auf der Extron-Website, www.extron.com.

Instrucciones de seguridad • Español

ADVERTENCIA: Este símbolo, , cuando se utiliza en el producto, avisa al usuario de la presencia de voltaje peligroso sin aislar dentro del producto, lo que puede representar un riesgo de descarga eléctrica.

ATENCIÓN: Este símbolo, , cuando se utiliza en el producto, avisa al usuario de la presencia de importantes instrucciones de uso y mantenimiento recogidas en la documentación proporcionada con el equipo.

Para obtener información sobre directrices de seguridad, cumplimiento de normativas, compatibilidad electromagnética, accesibilidad y temas relacionados, consulte la Guía de cumplimiento de normativas y seguridad de Extron, referencia 68-290-01, en el sitio Web de Extron, www.extron.com.

Instructions de sécurité • Français

AVERTISSEMENT : Ce pictogramme, , lorsqu'il est utilisé sur le produit, signale à l'utilisateur la présence à l'intérieur du boîtier du produit d'une tension électrique dangereuse susceptible de provoquer un choc électrique.

ATTENTION : Ce pictogramme, , lorsqu'il est utilisé sur le produit, signale à l'utilisateur des instructions d'utilisation ou de maintenance importantes qui se trouvent dans la documentation fournie avec le matériel.

Pour en savoir plus sur les règles de sécurité, la conformité à la réglementation, la compatibilité EMI/EMF, l'accessibilité, et autres sujets connexes, lisez les informations de sécurité et de conformité Extron, réf. 68-290-01, sur le site Extron, www.extron.com.

Istruzioni di sicurezza • Italiano

AVVERTENZA: Il simbolo, , se usato sul prodotto, serve ad avvertire l'utente della presenza di tensione non isolata pericolosa all'interno del contenitore del prodotto che può costituire un rischio di scosse elettriche.

ATTENZIONE: Il simbolo, , se usato sul prodotto, serve ad avvertire l'utente della presenza di importanti istruzioni di funzionamento e manutenzione nella documentazione fornita con l'apparecchio.

Per informazioni su parametri di sicurezza, conformità alle normative, compatibilità EMI/EMF, accessibilità e argomenti simili, fare riferimento alla Guida alla conformità normativa e di sicurezza di Extron, cod. articolo 68-290-01, sul sito web di Extron, www.extron.com.

Instrukcje bezpieczeństwa • Polska

OSTRZEŻENIE: Ten symbol, , gdy używany na produkt, ma na celu poinformować użytkownika o obecności izolowanego i niebezpiecznego napięcia wewnątrz obudowy produktu, który może stanowić zagrożenie porażenia prądem elektrycznym.

UWAGI: Ten symbol, , gdy używany na produkt, jest przeznaczony do ostrzegania użytkownika ważne operacyjne oraz instrukcje konserwacji (obsługi) w literaturze, wyposażone w sprzęt.

Informacji na temat wytycznych w sprawie bezpieczeństwa, regulacji wzajemnej zgodności, zgodność EMI/EMF, dostępności i Tematy pokrewne, zobacz Extron bezpieczeństwa i regulacyjnego zgodności przewodnik, część numer 68-290-01, na stronie internetowej Extron, www.extron.com

Инструкция по технике безопасности • Русский

ПРЕДУПРЕЖДЕНИЕ: Данный символ, , если указан на продукте, предупреждает пользователя о наличии неизолированного опасного напряжения внутри корпуса продукта, которое может привести к поражению электрическим током.

ВНИМАНИЕ: Данный символ, , если указан на продукте, предупреждает пользователя о наличии важных инструкций по эксплуатации и обслуживанию в руководстве, прилагаемом к данному оборудованию.

Для получения информации о правилах техники безопасности, соблюдении нормативных требований, электромагнитной совместимости (ЭМП/ЭДС), возможности доступа и других вопросах см. руководство по безопасности и соблюдению нормативных требований Extron на сайте Extron: www.extron.com, номер по каталогу - 68-290-01.

安全说明 • 简体中文

警告:  产品上的这个标志意在警告用户该产品机壳内有暴露的危险电压, 有触电危险。

注意:  产品上的这个标志意在提示用户设备随附的用户手册中有重要的操作和维护(维修)说明。

关于我们产品的安全指南、遵循的规范、EMI/EMF 的兼容性、无障碍使用的特性等相关内容, 敬请访问 Extron 网站, www.extron.com, 参见 Extron 安全规范指南, 产品编号 68-290-01。

安全記事・繁體中文

警告: ⚠ 若產品上使用此符號，是為了提醒使用者，產品機殼內存在著可能會導致觸電之風險的未絕緣危險電壓。

注意 ⚠ 若產品上使用此符號，是為了提醒使用者，設備隨附的用戶手冊中有重要的操作和維護（維修）說明。

有關安全性指導方針、法規遵守、EMI/EMF 相容性、存取範圍和相關主題的詳細資訊，請瀏覽 Extron 網站: www.extron.com，然後參閱《Extron 安全性與法規遵守手冊》，準則編號 68-290-01。

安全上のご注意・日本語

警告: この記号⚠が製品上に表示されている場合は、筐体内に絶縁されていない高電圧が流れ、感電の危険があることを示しています。

注意: この記号⚠が製品上に表示されている場合は、本機の取扱説明書に記載されている重要な操作と保守(整備)の指示についてユーザーの注意を喚起するものです。

安全上のご注意、法規遵守、EMI/EMF適合性、その他の関連項目については、エクストロンのウェブサイト www.extron.com より『Extron Safety and Regulatory Compliance Guide』(P/N 68-290-01) をご覧ください。

안전 지침・한국어

경고: 이 기호⚠가 제품에 사용될 경우, 제품의 인클로저 내에 있는 접지되지 않은 위험한 전류로 인해 사용자가 감전될 위험이 있음을 경고합니다.

주의: 이 기호⚠가 제품에 사용될 경우, 장비와 함께 제공된 책자에 나와 있는 주요 운영 및 유지보수(정비) 지침을 경고합니다.

안전 가이드라인, 규제 준수, EMI/EMF 호환성, 접근성, 그리고 관련 항목에 대한 자세한 내용은 Extron 웹 사이트(www.extron.com)의 Extron 안전 및 규제 준수 안내서, 68-290-01 조항을 참조하십시오.

Copyright

© 2018-2019 Extron Electronics. All rights reserved. www.extron.com

Trademarks

All trademarks mentioned in this guide are the properties of their respective owners.

The following registered trademarks (®), registered service marks (SM), and trademarks (TM) are the property of RGB Systems, Inc. or Extron Electronics (see the current list of trademarks on the [Terms of Use](#) page at www.extron.com):

Registered Trademarks (®)
Extron, Cable Cubby, ControlScript, CrossPoint, DTP, eBUS, EDID Manager, EDID Minder, Flat Field, FlexOS, Glitch Free, Global Configurator, Global Scriptor, GlobalViewer, Hideaway, HyperLane, IP Intercom, IP Link, Key Minder, LinkLicense, LockIt, MediaLink, MediaPort, NetPA, PlenumVault, PoleVault, PowerCage, PURE3, Quantum, Show Me, SoundField, SpeedMount, SpeedSwitch, StudioStation, System <i>INTEGRATOR</i> , TeamWork, TouchLink, V-Lock, VideoLounge, VN-Matrix, VoiceLift, WallVault, WindoWall, XTP, XTP Systems, and ZipClip
Registered Service Mark (SM): S3 Service Support Solutions
Trademarks (TM)
AAP, AFL (Accu-Rate Frame Lock), ADSP (Advanced Digital Sync Processing), Auto-Image, AVEdge, CableCover, CDRS (Class D Ripple Suppression), Codec Connect, DDSP (Digital Display Sync Processing), DMI (Dynamic Motion Interpolation), Driver Configurator, DSP Configurator, DSVP (Digital Sync Validation Processing), eLink, EQIP, Everlast, FastBite, FOX, FOXBOX, IP Intercom HelpDesk, MAAP, MicroDigital, Opti-Torque, PendantConnect, ProDSP, QS-FPC (QuickSwitch Front Panel Controller), Room Agent, Scope-Trigger, ShareLink, SIS, Simple Instruction Set, Skew-Free, SpeedNav, Triple-Action Switching, True4K, Vector™ 4K, WebShare, XTRA, and ZipCaddy

Conventions Used in this Guide

Notifications

The following notifications are used in this guide:

NOTE: A note draws attention to important information.

Specifications Availability

Product specifications are available on the Extron website, www.extron.com.

Extron Glossary of Terms

A glossary of terms is available at <http://www.extron.com/technology/glossary.aspx>.

Contents

Introduction	6
Overview.....	6

Topology.....	7
----------------------	----------

Prerequisites.....	9
Security Certificates	9
Certificate File Requirements	9
Private Key File Requirements	10
Supported Authentication Protocols.....	11
EAP-TLS Requirements.....	11
PEAP-MSCHAPV2 Requirements	11

Configuring an Extron Device	12
Step 1 — Enabling 802.1X on an Extron Device	12
Step 2 — Connecting an Extron Device to an 802.1X Network.....	13
Step 3 — Validating 802.1X Authentication of the Extron Device.....	14

Troubleshooting	15
Certificate Manager Messages	16
Event Log Security Messages.....	17

Glossary	19
-----------------------	-----------

Introduction

This reference guide is part of a collection of documents that cover different aspects of 802.1X support for Extron devices. Reference each as necessary.

- **802.1X Primer White Paper** — a synopsis for the implementation and support of the 802.1X feature
- **Security section of the Toolbelt help file** — a step-by-step instructional guide for setting up and troubleshooting Extron devices for use on an 802.1X network
- **802.1X Technology Reference Guide (this document)** — a high-level guidebook to the 802.1X technology with general setup and troubleshooting instructions.

This reference guide provides a general overview of the 802.1X networking standard, prerequisites for setting up Extron devices using the 802.1X standard, and basic troubleshooting information. This document is meant to be used as a reference guide for Extron products that support 802.1X. For other general information on 802.1X, visit the IEEE Standard Association web site or consult with your IT department.

This section provides a brief introduction to the 802.1X networking standard.

Overview

IEEE 802.1X is a networking standard that enables port-based network access control via an authentication server. The protocol requires that all Extron devices that wish to connect to the secure side of the network get authenticated before gaining any network privileges.

802.1X authentication involves three parties:

- **Supplicant** — a user or device that requests access to a network that supports 802.1X
- **Authenticator** — a device (switch or Wireless Access Point [WAP]) that controls the supplicant network access to the LAN/VLAN. The authenticator acts as an intermediary between the supplicant and the authentication server; during the authentication process, it transmits information from one entity to the other until the authentication server sends an authentication resolution. If the authentication is successful, the switch port becomes authorized. If unsuccessful, the port is restricted and is either left without network access, or re-directed to VLAN with limited services.
- **Authentication Server** — a device that grants or denies network access to the supplicant. In the authentication process, the authentication server validates the identity of the supplicant and notifies the authenticator whether or not the supplicant is allowed to use the network.

Topology

Thanks to the new Extron 802.1X implementation, the Extron IPL Pro Control Processors can now be configured as supplicants on a privileged (secure) infrastructure. Before connecting the control processors to a network with 802.1X support, these devices must be configured via Extron Toolbelt software. Once authenticated successfully, the control processors are able to join and communicate on the network. The Extron 802.1X Topology figure on the next page shows the different configurations that can be achieved through the Extron 802.1X implementation.

- For simple use, any IPL Pro Control Processor can be configured as a supplicant and connected to the 802.1X network via LAN. The IPCP Pro 250 in the 802.1X Topology figure is configured and connected in this manner.
- For a more compound use, controllers with AV LAN features can be configured as supplicants and connected to the 802.1X network via LAN. The devices connected on the AV LAN are in their own (secluded) network, and therefore are not considered to be supplicants. The IPCP Pro 255, along with the connected AV LAN devices (IPL Pro S3 and TLP Pro 725M) in the 802.1X Topology figure are configured in this manner.
- For a more utilitarian use, a control processor with an embedded LAN switch can be configured as a supplicant. More supplicants can be connected to the device to increase the number of authorized devices per 802.1X port. The IPCP Pro 350 in the 802.1X Topology figure is configured in this manner.

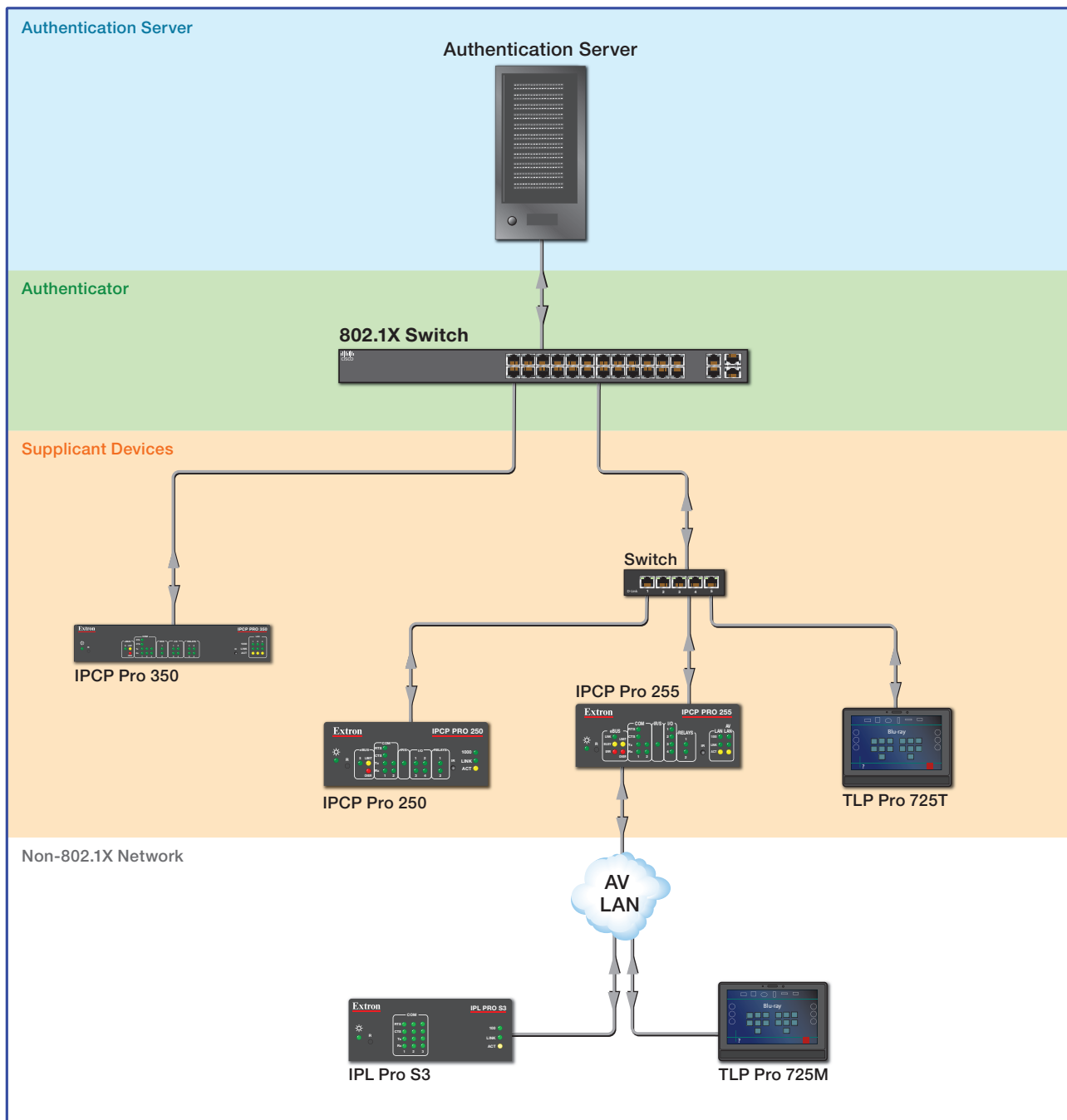


Figure 1. 802.1X Topology

Prerequisites

This section contains information regarding the elements that are needed prior to configuring Extron devices for 802.1X.

- [Security Certificates](#)
- [Supported Authentication Protocols](#)

Security Certificates

Security certificates are electronic documents which contain information that uniquely identifies each certificate owner. Depending on the intended method of authentication and the network requirements, these certificates may be required in order to set up 802.1X authentication on Extron products.

Certificate and private key files to be loaded to Extron devices must adhere to the X.509 standard. This standard specifies both the format and information the certificate must have. For more information regarding X.509 certificates, consult with the International Telecommunications Union (ITU) website.

Certificate File Requirements

- Valid Certificate File extensions: .pem, .crt
- If .pem, the code inside the file should resemble:

```
-----BEGIN CERTIFICATE-----  
[Certificate File content]  
-----END CERTIFICATE-----
```

The box and the software might prevent the user from loading certificates that have metadata (lines or characters above and below the “--BEGIN...” and “--END...” lines) in them. If you have any trouble loading a .pem certificate, open a text editor (like Notepad ++) and check the file for:

- Empty lines above or below the “--BEGIN...” and “--END...” lines
- Information or extra characters above and below the “--BEGIN...” and “--END...” lines

NOTE: DER encoded files (files with the following extensions: .der, .crt, .cer and encoded in DER binary) must be converted to a PEM encoding file type (.pem) before being utilized for authentication.

- The file name **MUST** be 5-128 characters long, and **CAN** include:
 - Alphanumeric characters (A-Z, a-z & 0-9)
 - The following special characters: period (.), underscore (_), hyphen (-)
- Certificate types:
 - Certificate Authority
 - Machine

CA Certificate requirements

Digital certificates are issued by a Certificate Authority (CA) to validate a trusted server and its identity on the supplicant (client) end. For CA Certificates, the trusted path of root (and, if applicable, intermediate) certificates must be loaded to the Extron device in a single file.

Also, when using CA certificates, the Extron device date and time must be set up correctly. Incorrect date and time settings can cause authentication failure.

Currently .crt, and .pem are the only acceptable file extensions for these certificate files. Consult other file requirements in the certificate file requirement section.

Private Key File Requirements

Private key files are used in the encryption/decryption of data sent between the server and connecting clients. Private key files and Certificate Signing Requests (CSR) have a one-to-one correspondence. Certificates generated with a particular CSR, will only work with the corresponding private key file. All machine certificates require their corresponding private key file to work.

- Valid certificate file extensions: .pem, .key
- If .pem, the code inside the files should resemble:
 - If encrypted:

```
-----BEGIN ENCRYPTED PRIVATE KEY-----  
[Private Key File content]  
-----END ENCRYPTED PRIVATE KEY-----
```

- If not encrypted:

```
-----BEGIN RSA PRIVATE KEY-----  
[Private Key File content]  
-----END RSA PRIVATE KEY-----
```

The box and the software might prevent the user from loading certificates that have metadata (lines above and below the “–BEGIN...” and “–END...” lines) in them.

If you have any trouble loading the certificate check the file for:

- empty lines above or below the “–BEGIN...” and “–END...” lines
- Information or extra characters above and below the “–BEGIN...” and “–END...” lines

NOTE: DER encoded files (files with the following extensions: .der and encoded in DER binary) must be converted to a PEM encoding file type (.pem) before being utilized for authentication

- The file name MUST be 5 - 128 characters long, and CAN include:
 - Alphanumeric characters (A-Z, a-z & 0-9)
 - The following special characters: period(.), underscore(_), hyphen(-)

Supported Authentication Protocols

EAP-TLS and PEAP-MSCHAPV2 are the two authentication protocols supported by Extron products. Each protocol requires different information to be set up successfully.

Use the Extron Toolbelt software to complete the individual setup of the desired supplicants (see [Configuring an Extron Device](#) on the next page). For detailed instructions on how to manage certificates and how to set up 802.1X on Extron products, see the *Toolbelt Help* file.

EAP-TLS Requirements

- **Identity** (as stored in the Active Directory)
- **Supplicant certificate**
- **CA certificate** (optional)

PEAP-MSCHAPV2 Requirements

- **Anonymous identity** (optional)
- **PEAP-MSCHAPV2 version number**
- **Username** (as stored in the Active Directory)
- **Password** (as stored in the Active Directory)
- **CA certificate** (optional)

Configuring an Extron Device

This section contains an overview of the 802.1X setup process for Extron devices.

- **Step 1 — Enabling 802.1X on an Extron Device**
- **Step 2 — Connecting an Extron Device to an 802.1X Network**
- **Step 3 — Validating 802.1X Authentication of the Extron Device**

Step 1 — Enabling 802.1X on an Extron Device

Extron devices must be set up on a non-802.1X network prior to connecting to a network with 802.1X authentication support.

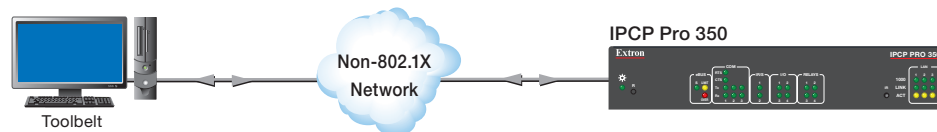


Figure 2. Enabling 802.1X on an Extron Device

Before attempting to enable 802.1X, ensure that Extron device and PC are on the same non-802.1X network

To enable 802.1X:

1. Manage the Extron device within the Toolbelt software.
2. On the **Security** tab, check the **Enable IEEE 802.1X Authentication** checkbox (see the *Toolbelt Help* file for more details).
3. After applying the settings, reboot or power-cycle the Extron device.

Step 2 — Connecting an Extron Device to an 802.1X Network

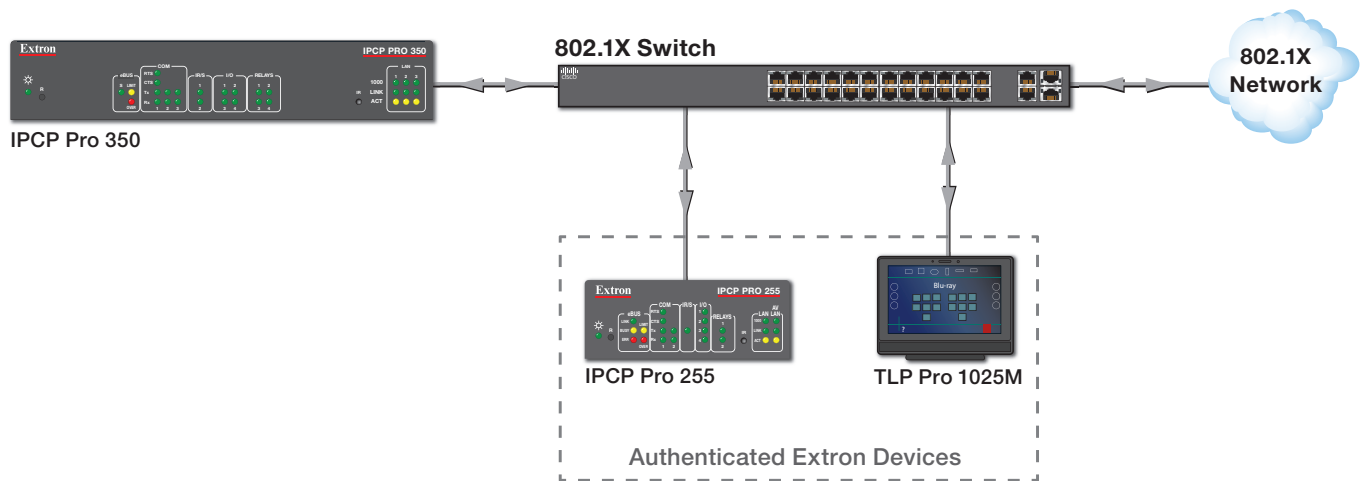


Figure 3. Connecting an Extron Device to an 802.1X Network

Before attempting to connect to an 802.1X network, ensure that:

- The Extron device currently has 802.1X enabled
- 802.1X security certificates and settings were successfully applied to the Extron device

To connect to an 802.1X network:

1. Disconnect the Extron device from the current non-802.1X network.
2. Connect the Extron device to the 802.1X network.

Step 3 — Validating 802.1X Authentication of the Extron Device

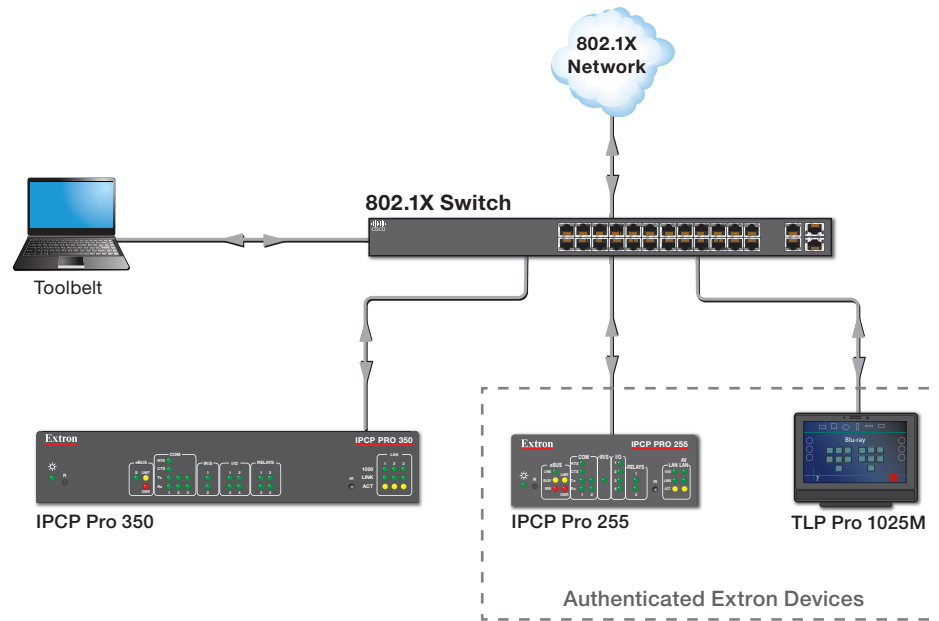


Figure 4. Validating 802.1X

An authenticated PC running the Toolbelt utility can validate whether or not the 802.1X setup was successful. Figure 4 shows a basic setup for validating 802.1X on a Extron device.

Before validating the 802.1X authentication, ensure that:

- The Extron device and the PC are connected to the 802.1X network
- 802.1X security certificates and settings were successfully applied

To validate the 802.1X authentication:

1. Open the Toolbelt software on the PC.
2. Go to the **Logs** tab and check the Event Logs for a Successful Authentication message.
or
Go to the **Utilities** tab and use the Proxy Ping utility to ping Extron devices that are already authenticated on the same 802.1X network (see the *Toolbelt Help* file for more information).

Troubleshooting

NOTE: Please use the latest versions of firmware and Toolbelt to enable access to the **Security** tab, which allows users to enable IEEE 802.1X authentication and manage certificates.

This section contains basic troubleshooting information. Most of the 802.1X troubleshooting can be done from within the Toolbelt software. Many of the error and authentication messages are displayed in the supplicant **Logs** and **Security** tabs. The messages displayed are the most helpful way for a user to obtain information about failed authentications.

If experiencing difficulties during the authentication process and no message is displayed in the event logs, try the network and device settings troubleshooting techniques listed below.

- If a device cannot authenticate and all 802.1X settings appear correct:
 - The authentication process can take a minute or two to complete. Make sure to give enough time for the logs to show the status. Interrupting the authentication process by unplugging the network cable too soon may cause unexpected failures.
 - Check the supplicant event log messages for more information.
- If event logs are not displayed:
 - Check the supplicant general settings for any errors.
 - If using CA and machine certificates, verify that the supplicant date and time settings match the system settings. Incorrect date and time information can cause issues with the validity period of a certificate.
 - When setting up an Extron device for 802.1X, verify the supplicant network settings. IP address, subnet mask, and gateway IP addresses are fundamental for communication with the authenticator and the authentication server.
 - Check the LINK LED on the device.
 - If not blinking, the port request might have been rejected and the device is “Not Authorized” on the network. Power cycle the device to re-attempt authentication.
 - If blinking, the device is exchanging communication packages. Power cycle the device and check for event log messages.

The following tables contain the error messages related to 802.1X and possible resolutions. If the procedures in this section do not resolve the problem, contact your technical support team for further network troubleshooting help. If additional help is necessary, contact Extron support.

Certificate Manager Messages

Message	Possible Cause	Possible Resolution
Upload successful	Attempt to upload certificate succeeded	
Your settings were saved successfully	All settings saved successfully	
We were unable to upload your certificate. Please check the file and try again.	• Key filename or certificate contains invalid characters • Key filename or certificate filename length error • Private key file or Certificate file contains unknown label header or footer • File provided is a certificate request and not a certificate.	Confirm that your certificate or private key file name only contains: • Alphanumeric characters A-Z, a-z, 0-9 • Special characters: period, colon, underscore, hyphen • Is within the character length limit (5-128 characters) Confirm that your certificate or private key file: • Contains the expected file extension (.crt, .pem, .key) • Contains a valid PEM encoded header and footer (BEGIN and END lines with no extra characters above or below)
Certificate file does not follow security requirements	• Certificate is incorrectly formatted • Certificate is not a PEM encoded file • Certificate has wrong number of characters per line • Missing or corrupt label (first and last line)	Confirm that your certificate follows certificate file requirements or contact the person who supplied the files
Private key file does not follow security requirements		
Private key file password is not correct	• Private key password input incorrectly • Incorrect password for the private key file	• Correct the password in the certificate manager • Confirm the password and the private key file belong together
Certificate and private key files do not match	• Private key and password are okay but do not go together	Confirm the certificate and private key file belong together

Event Log Security Messages

ID	Message	Possible Cause	Possible Resolution
1103	<Machine Certificate File Name> with alias <Alias>: Certificate Upload Successful	Machine certificate was successfully loaded onto the Extron device.	
1104	<Machine Certificate File Name> with alias <Alias>: Certificate Removed	CA or machine certificate was removed from the Extron device and replaced by a new one.	
1107	<CA Certificate File Name> with alias <Alias>: Certificate Removed		
1105	<Machine Certificate File Name> with alias <Alias>: Certificate Removed		
1108	<CA Certificate File Name> with alias <Alias>: Certificate Removed	CA or machine certificate was removed from the Extron device.	
1106	<CA Certificate File Name> with alias <Alias>: Certificate Upload Successful		
1201	802.1X authentication successful	Extron device authenticated successfully on the intended network.	
1202	802.1X authentication Failed: Invalid user credential	Username/password for the loaded certificate may: • Be inputted incorrectly • Not match the credentials stored on the network Loaded certificate may be: • Corrupted • Registered to an unauthorized user on the network	Confirm credentials (username, password, or machine certificate) are correct, and if needed, re-upload and re-apply.
1203	802.1X authentication Failed: Authentication server identity does not match the expected identity	Loaded certificate may: • Not be issued by a trusted Certificate Authority • Have a broken certificate path	• Confirm appropriate CA certificate is used. • Ensure all necessary certificates are used in the file.
1204	802.1X authentication Failed: The supplicant is not on 802.1X network	Extron device failed to get a resolution from the 802.1X network within the set time frame.	

ID	Message	Possible Cause	Possible Resolution
1221	<CA <i>Certificate File Name</i> > with alias <Alias>: Certificate Expired	Authentication date has exceeded certificate expiration date.	• Confirm the expiration date on the certificate. • Confirm the appropriate date and time settings on the Extron device.
1222	<Machine Certificate File Name> with alias <Alias>: Certificate Expired		
1223	<Machine <i>Certificate File Name</i> > with alias <Alias>: Certificate Expired		
1230	802.1X is disabled and reboot required	802.1X was disabled manually.	Reboot the device to complete the operation.

Glossary

Active Directory — Directory service that enables centralized and secured management of network resources.

Authentication Server — Device that grants or denies network access to the supplicant. In the authentication process, the authentication server validates the identity of the supplicant and notifies the authenticator whether or not the supplicant is allowed to join the network.

Authenticator — Device (switch or Wireless Access Point) that controls the supplicant network access to the LAN/VLAN. The Authenticator acts as an intermediary between the supplicant and the authentication server; during the authentication process, it transmits information from one entity to the other until the authentication server sends an authentication resolution. If the authentication is successful, the switch port becomes authorized. If unsuccessful, the port is restricted either left without network access or it gets re-directed to VLAN with limited services. This may vary depending on IT network policy.

CA Certificate — Digital certificate issued by a Certificate Authority to validate a trusted server identity on the supplicant (client) end. For CA Certificates, the trusted path of root (and, if applicable, intermediate) certificates must be loaded to the device in a single file.

Certificate Path — Visual representation of the chain of trusted certificates from the supplicant to one root with one or more Intermediate certificates in between

EAP-TLS — Extensible Authentication Protocol - Transport Layer Security (EAP-TLS) is an authentication framework that uses a TLS session with digital certificates to carry on authentication between the client and authentication server .

IEEE 802.1X — Institute of Electrical and Electronics Engineers (IEEE) standard that enables port-based Network Access Control (PNAC). The standard provides a mechanism for client devices, upon request and approval, to communicate on the “secure” side of any configured LAN or WLAN.

Machine Certificate — Digital certificate that has information about the authenticity and identity of a device or workstation, so that the identity of the Extron device can be validated. Machine certificates generated for our devices must be assigned a unique alias, and have a private key file and a private key password*. Currently .crt, and .pem are the only acceptable file extensions for certificate files.

NOTE: *The password can be an empty password if the private key is not encrypted.

Private Key File — File used in the encryption/decryption of data sent between the server and connecting clients. Private key files and Certificate Signing Requests (CSR) have a one-to-one correspondence. Certificates generated with a particular CSR, will only work with the corresponding private key file. All machine certificates require their corresponding private key file to work.

Private Key Password — The second layer of security to the EAP-TLS method. This password is used to protect the supplicant private key.

- Optional (0 - 256 characters)
- All ASCII printable characters

Protected EAP (PEAP) — Protected Extensible Authentication Protocol (PEAP). Authentication framework that uses directory services credentials (username/password) to grant or deny access to supplicant devices wishing to communicate in an 802.1X enabled network.

Supplicant — A user or device that is requesting access to a network that supports 802.1X.

Supplicant Certificate — The machine certificate and private key set loaded on the device to identify the Extron device/workstation as an authorized user/machine in the network supporting 802.1X.

