CRESTRON SECURE DEPLOYMENT GUIDE

Crestron Engineering

7/18/2016

Instructions for creating a secure installation using Crestron equipment.

Version	Date	Notes	Author
1.00	February 23, 2015	Release Version	JP
1.01	March 13, 2015	Added Web Server Information	JP
1.02	March 23, 2015	Added disabling of TSW Setup Key Sequence	JP
1.03	May 6, 2015	Added information regarding Remote Access	JP
1.04	June 9, 2015	Corrected CIPHER command	JP
1.05	April 22, 2016	Updated to 1.5xx firmware (keep SSH enabled) and addition of DM Matrix Switch Information	JP
1.06	July 18, 2016	Added SECUREGATEWAYMODE information	JP

TABLE OF CONTENTS

OVERVIEW

This document describes the steps needed to harden a Crestron installation.

This document assumes a basic understanding of security functions and protocols.

This document references the following devices and versions.

3-Series Control System	1.5xx
DMPS3	1.5xx
TSW-xx2 Touch Screen	1.002.xxx

SUGGESTED SYSTEM CONFIGURATION

Crestron devices are created using a variety of platforms and processors. In some cases, devices are unable to provide the full set of security features that might be needed for some solutions.

Crestron's CP3N, AV3, and PRO3 all feature the Crestron Control Subnet, which is an easy way to create a new Ethernet network dedicated to Crestron's Ethernet devices. The Control Subnet's main purpose is to simplify setting up a dedicated Crestron LAN. As such, the Control Subnet has a DHCP and DNS Server. The Control Subnet is designed as a fully functional firewall/router, and the control system and Crestron tools will open up ports as needed.

By default, the devices on the Control Subnet are able to reach out to the wider LAN. But, other traffic inbound into the Control Subnet is limited to Crestron tools.

To further restrict the system, the 3-Series processor supports ISOLATION MODE. In this MODE, the firewall is configured in such a way that NO traffic can traverse from the LAN to the devices on the Control Subnet, nor from the Control Subnet to the LAN.

Using this mechanism, customers can protect their corporate LAN from devices on the Control Subnet.

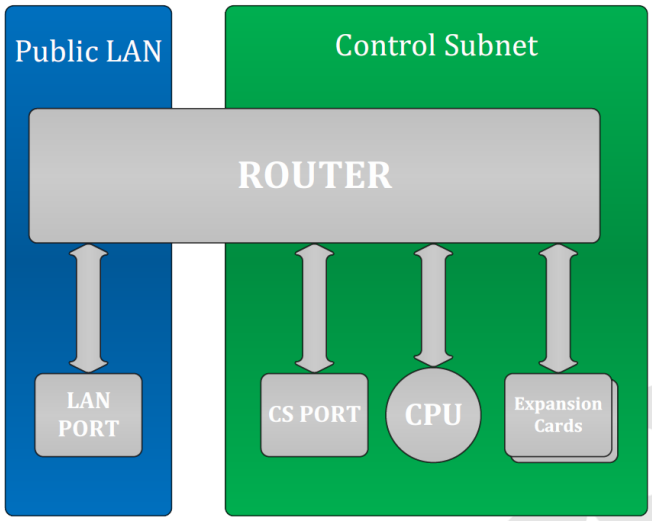
ARCHITECTURE

Even if nothing is plugged into the Control Subnet port on the back of the control system, there are still some devices on the Control Subnet:

- Control System CPU (This is where the AV Programs run)
- Optional Expansion cards (PRO3 and AV3 only)

This design is in place to make sure that the Crestron CPU and optional expansion cards are protected from malicious packets on the LAN.

Please see this diagram for clarification how all the components work together.



The firewall rules only allow in the traffic that the CPU is listening to. As such, a port scan will only show ports that the CPU is listening to. Users have the ability to set up manual port forwarding rules to make custom connections to the devices on the Control Subnet.

Crestron's management utility, Crestron Toolbox, creates custom port forwarding rules in the 64000–64299 range to enable management of the devices on the Control Subnet. These port forwarding rules are created when the tool connects and are broken down when the tool disconnects or when the device is rebooted.

FIREWALL RULES IN NORMAL OPERATION

Under normal operation procedures, the firewall on the CS Router is set as follows:

DIRECTION	PORT	RULE	DESCRIPTION
Inbound from LAN	20 & 21	To CPU	FTP (if enabled)
Inbound from LAN	22	To CPU	SSH
Inbound from LAN	23	To CPU	Telnet (if enabled)
Inbound from LAN	80 & 443	To CPU	Web (if enabled)
Inbound from LAN	843	To CPU	Flash Policy (if enabled)
Inbound from LAN	41794–41797	To CPU	Crestron communication protocols
Inbound from LAN	Listen Ports used by program	To CPU	Programmatic listeners
Inbound from LAN	64000–64299	To Devices on CS	Allowing Crestron Management tool to access the devices on the Control Subnet. These ports are opened and closed as needed.
Control Subnet outbound to LAN	Any Port	Allowed	All outbound traffic is allowed
Inbound from LAN	User defined	User Defined	This allows the end-user to do manual port forwarding to devices on the Control Subnet.

FIREWALL RULES IN ISOLATION MODE

When ISOLATION MODE is enabled, the rules are as such:

DIRECTION	PORT	RULE	DESCRIPTION
Inbound from LAN	20 & 21	To CPU	FTP (if enabled)
Inbound from LAN	22	To CPU	SSH
Inbound from LAN	23	To CPU	Telnet (if enabled)
Inbound from LAN	80 & 443	To CPU	Web (if enabled)
Inbound from LAN	843	To CPU	Flash Policy (if enabled)
Inbound from LAN	41794–41797	To CPU	Crestron communication protocols
Inbound from LAN	Listen Ports used by program	To CPU	Programmatic listeners
Inbound from LAN	64000–64299	BLOCKED	In ISOLATION MODE, even Crestron's tools cannot connect to any devices on the Control Subnet
Control Subnet outbound to LAN	Any Client Ports used by program	From CPU: Allowed	
Control Subnet outbound to LAN	Any Port	All other devices: BLOCKED	No outbound traffic is allowed
Inbound from LAN	User defined	BLOCKED	In ISOLATION MODE, no port forwarding can be managed by the user

On top of the firewall rules, ISOLATION MODE also disables the functionality needed for making port mappings by either the user or Crestron tools. Therefore, in ISOLATION MODE, not even Crestron's tools can connect to the devices on the Control Subnet.

The only device that can communicate with both the LAN and the Control Subnet in ISOLATION MODE is the Control System CPU.

ASSUMPTIONS

1. The system is not capable of dual authorization. If your organization policy requires this, you cannot use this system.
2. Physical security, commensurate with the value of the system and the data it contains, is assumed to be provided by the environment.

3. Administrators are trusted to follow and apply all administrator guidance in a steadfast manner.

COMMON STEPS

1. Input the command 'AUTH ON'. You will be prompted for the name and password of an Administrator account. DO NOT LOSE THIS INFORMATION. THE SYSTEM CANNOT BE ACCESSED WITHOUT THIS INFORMATION.
2. Create other users and assign them to groups as desired. More information is in the section More About User Groups.
3. Input the command 'CIPHER STRONG'.
4. If your installation requires Banners, please copy the Banner to the following device folder: /SSHBanner/banner.txt.

At this time, FTP, HTTP, and TELNET services will be disabled.

HTTPS will continue to be available.

OPTIONAL STEPS

The steps below are all optional. The reasons for performing or not performing these steps are also provided.

SECURE CONNECTIONS

With authentication and TLS enabled, devices may optionally connect using these secured methods, but by default, devices may also connect using unsecured communications.

This may be configured using the command 'SECUREGATEWAYMODE'. The following parameters are supported.

- DEFAULT – Accepts both secure and unsecure Gateway CIP connections on all network interfaces.
- SECUREONLY – Accepts only secure Gateway CIP connections on all network interfaces.
- SECURENONCS - (Only valid for the CP3N, PRO3, AV3) Accept secure and unsecure Gateway CIP connections from devices on the control subnet but only secure connections will be accepted on the LAN interface.
- SECUREEXT - Accept only secure Gateway CIP connections from external IP addresses (i.e. from different subnets than any of the connected networks). Accepts unsecure connections from IP addresses on the same subnet as the given network interface (i.e. LAN port allows unsecure connections on the local LAN subnet, Control Subnet port allows unsecure connections from its local subnet). This is a good selection to ensure that all mobile devices are properly configured to use TLS/SSL communications.

WEB SERVER

Crestron Control Systems contain a built-in Web Server. When SSL/TLS is enabled, port 80 will remain open but will ONLY redirect to port 443. The Web Server will then prompt for authentication credentials.

If the Web Server is not being used, some customers may prefer to disable it entirely.

```
WEBSERVER [ON | OFF]
```

No parameter - displays current setting

SET LOCK OUT CONFIGURATION

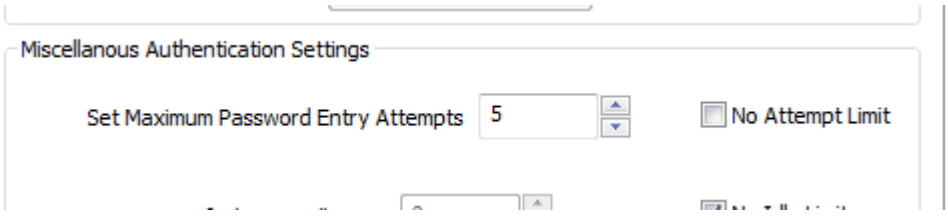
Rationale: To prevent brute force attacks, the system only allows a certain number of attempts before locking out the source IP address. By default, 3 unsuccessful attempts from the same IP address will block that address for 24 hours. A more secure installation would not allow automatic unlocks as this allows potential attackers to retry possible user password combinations without the knowledge of the user or the administrator.

```
PRO3>setloginattempts ?
SETLOGINAttempts [number]
```
`number`: number of logon attempts a user will have before the console is blocked, 0 is infinite
No parameter: display current setting

```
PRO3>setlockouttime ?
SETLOCKOUTTIME [number]
```
`number`: number of hours to block an IP address, 0 is indefinite, 255 max
No parameter: display current setting

For USB transport, the transport is blocked for 5 seconds after the maximum number of logon attempts is reached. If the user tries again after 5 seconds and continues to fail, the block time is doubled. The block time continues to be doubled until a successful logon or a control system reboot happens. Once a user successfully authenticates against the console, the failure count is reset to 0 and the block time is reset to 5 seconds.

This can be set in Crestron Toolbox from the Authentication Settings dialog.



BLOCKED IP ADDRESS FUNCTIONS

When a user reaches the maximum number of logon attempts over an Ethernet Connection (CTP/SCTP/SSH), the client's IP address is blocked. Administrators have access to commands that allow them to manage this behavior.

CHANGE LOCK OUT TIME

To change the number of hours an IP address is blocked, use the following command:

`SETLOCKOUTTIME [number]`

`number`: number of hours to block an IP address, 0 is indefinite, 255 max

No parameter: display current setting

LIST BLOCKED IP ADDRESSES

`LISTBLOCKEDip`

No parameter: display current list of blocked IP addresses

ADD AN IP ADDRESS TO THE BLOCKED LIST

`ADDBLOCKEDip [ipaddress]`

`ipaddress`: IP address to block

No parameter: display current list of blocked IP addresses

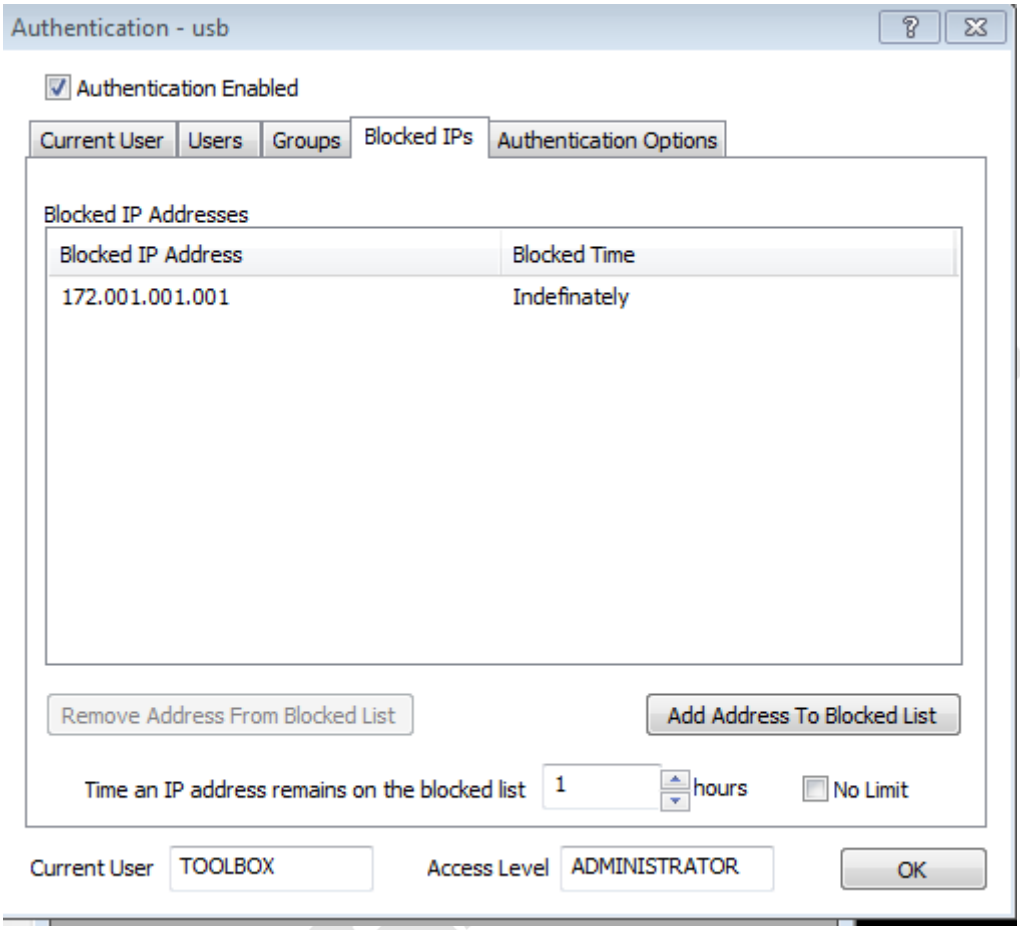
REMOVE AN IP ADDRESS FROM THE BLOCKED LIST

`REMBLOCKEDip [ALL|ipaddress]`

`ipaddress`: IP address of the blocked connection

`ALL`: remove all blocked IP addresses

No parameter: display current list of blocked IP addresses



SET PASSWORD RULES

Rationale: Installations may have individual password rules that need to be applied.

```
SETPASSWORDRULE {-ALL | -NONE} | {-LENGTH:minPasswordLength} {-
MIXED} {-DIGIT} {-SPECIAL}
```

-ALL: all rules will be applied.

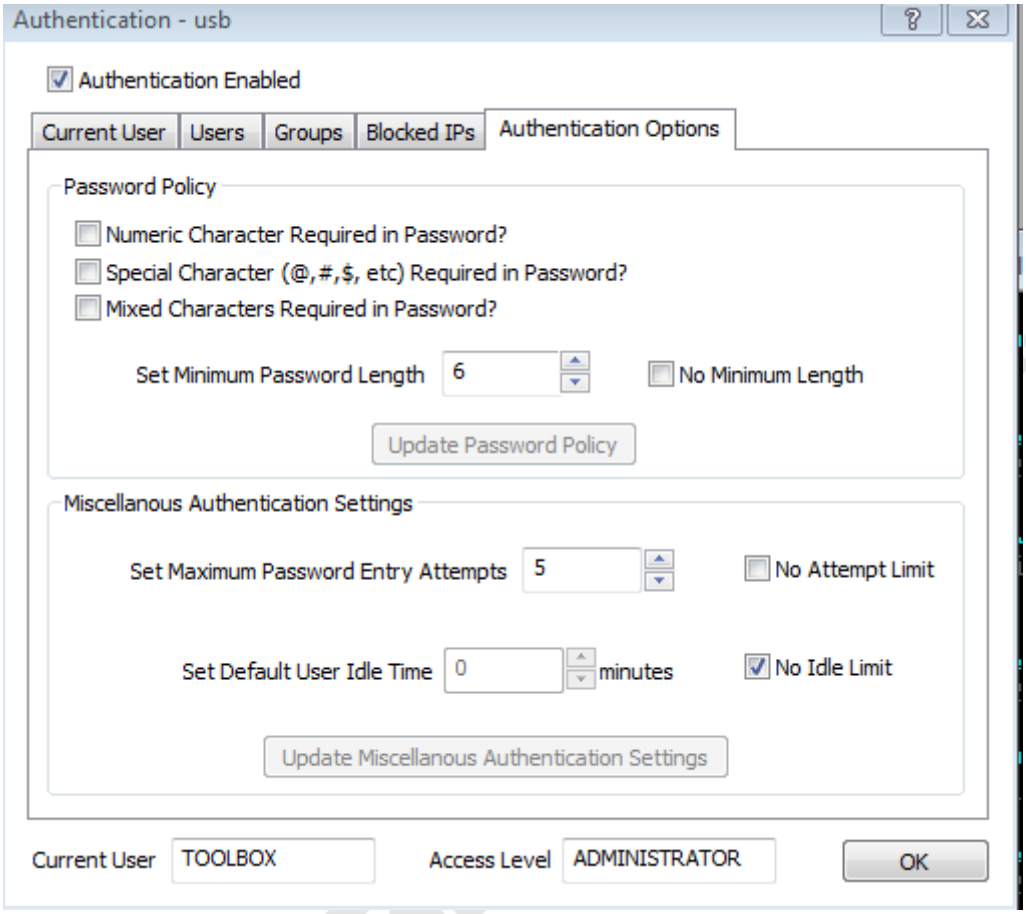
-NONE: no rules will be applied.

-LENGTH: specifies minimum password length. By default, the minimum length is 6. This parameter can't be combined with NONE.

-MIXED: password must contain a lower and upper case character. This parameter can't be combined with NONE.

-DIGIT: password must contain a number. This parameter can't be combined with NONE.

-SPECIAL: password must contain a special character. This parameter can't be combined with NONE.



OTHER PASSWORD COMMANDS

CHANGE LOCAL USER PASSWORD

When authentication is on, any logged-in user can change his or her password. The user is prompted to enter the old password once and the new password twice. If the old password does not match the current password, this operation fails and the password is not changed.

`UPDATEPASSWORD`

No parameters needed

RESET LOCAL USER PASSWORD

When authentication is on, users with administrator rights can reset a user's password.

`RESETPASSWORD -N:username -P:defaultpassword`

`-N`: specifies name of the user to be reset

`-P`: specifies the default password

AUTHENTICATE USING ACTIVE DIRECTORY

ADD LOCAL OR ACTIVE DIRECTORY USER TO A LOCAL GROUP

Local users are created on 3-Series Control Systems without any access rights. By adding them to a local group, they inherit the access level from the group. A 3-Series Control System cannot create or remove a user from Active Directory but it can grant access to an existing user in Active Directory. To grant access to an Active Directory user, either add the user to a local group on the control system or add the Active Directory group(s) that the user is a member of to the control system.
When authentication is turned on, users with administrator rights can perform this operation.
`ADDUSERTOGROUP -N:username -G:groupname`
`-N:` specifies name of a local or domain (domain\user) user
`-G:` specifies name of a local group

REMOVE LOCAL OR ACTIVE DIRECTORY USER FROM A LOCAL GROUP

When authentication is turned on, users with administrator rights can perform this operation. After users are removed from a local group, they are deprived of the access rights associated with the group. The user account is not deleted by this command.
`REMOVEUSERFROMGROUP -N:username -G:groupname`
`-N:` specifies name of a local or domain user
`-G:` specifies name of a local group

ADD ACTIVE DIRECTORY GROUP

A 3-Series Control System cannot create or remove a group from Active Directory but it can grant access to an existing group in Active Directory. When authentication is on, users with administrator right can add an Active Directory group to the control system and assign certain access level. Once the group is added, all members of the group have access to the control system.
`ADDDOMAINGROUP -N:groupname -L:accesslevel`
`-N:` specifies the domain group name (domain\group)
`-L:` specifies one of the following access levels:
`A:` - as an Administrator
`P:` - as a Programmer
`O:` - as an Operator
`U:` - as a User
`C:` - for Connection only

DELETE ACTIVE DIRECTORY GROUP

When authentication is on, users with administrator rights can remove a previously added Active Directory group from the control system. The group is not deleted from Active Directory. Once the group is removed from the control system, all members of that group lose access to the control system.
`DELETEDOMAINGROUP domaingroupname`
`domaingroupname`: name of the domain group (domain\groupname) to be deleted.

LIST USERS

This command allows users with administrator rights to list all the users (local and domain) added to the

local groups.
LISTUSERS
No parameters needed.

LIST GROUP USERS

This command allows administrators can see a list of all users in a specified group.
LISTGROUPUSERS groupname

LIST LOCAL GROUPS

Users with administrator rights can list all the local groups added to the control system. A 3-Series Control System comes with the following built-in groups, which cannot be deleted by any user: Administrators, Programmers, Operators, Users, and Connects.
LISTGROUPS [A] [P] [O] [U] [C]
A: groups with administrator rights are listed
P: groups with programmer rights are listed
O: groups with operator rights are listed
U: groups with user rights are listed
C: groups with connection rights are listed
No parameter: all groups are listed

LIST ACTIVE DIRECTORY GROUPS

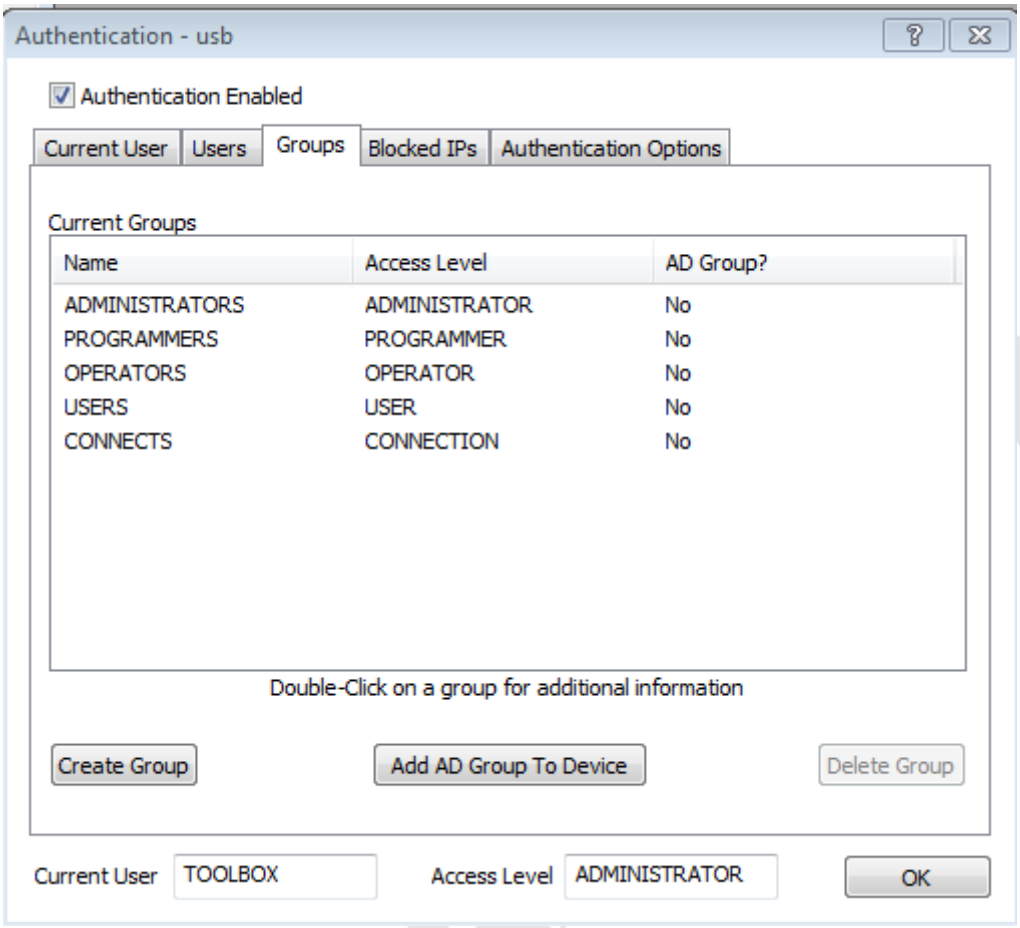
Users with administrator rights can list all the Active Directory groups that were added to the control system.
LISTDOMAINGROUPS [A] [P] [O] [U] [C]
A: groups with administrator rights are listed
P: groups with programmer rights are listed
O: groups with operator rights are listed
U: groups with user rights are listed
C: groups with connection rights are listed
No parameter: all groups are listed

SHOW USER INFORMATION

Administrators can query the controller to show the access rights of a particular user.
USERINFOrmation username

WHO COMMAND CHANGE

When Authentication is enabled, the WHO command also shows the currently logged-in users. This is in addition to what it currently lists. The list is filtered base on access level (lower access cannot see higher access).
WHO



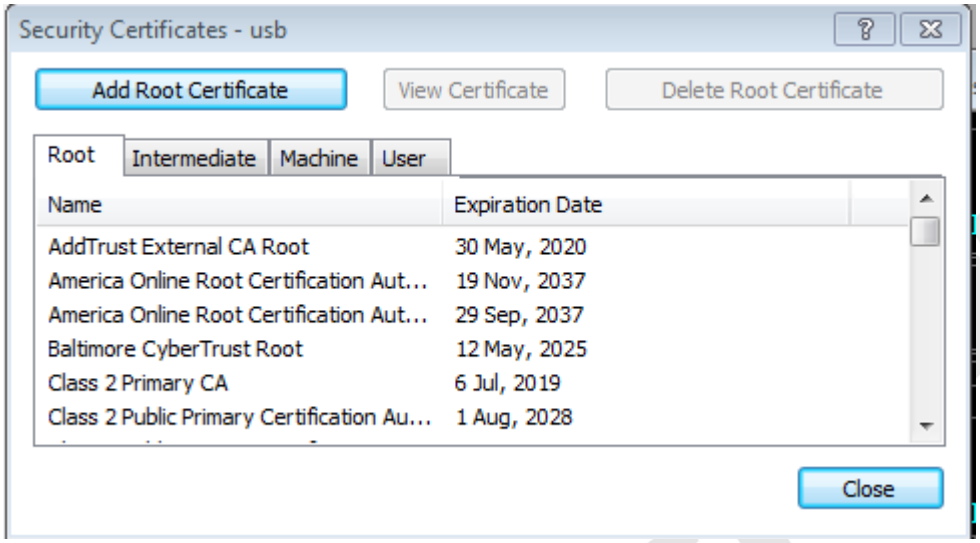
INSTALL A CERTIFICATE

Rationale: The certificate created when authentication is enabled is self-signed. A certificate from a trusted root authority might be needed in some installations.

```
PRO3>certificate ?
CERTIFicate Cmd Certificate_Store <Certificate_Name> <Certificate_UID>
<Password>
      Where Cmd = [ADD|REM|LIST|VIEW]
      Where Certificate_Store = [ROOT|MACHINE|USER|INTERMEDIATE]
      ADD  Certificate_Store -                  Add Certificate(from
known location) To Spedified Certificate Store (MACHINE store requires
password)
      REM  Certificate_Store Certificate_Name Certificate_UID -
Remove Specified Certificate From Specified Certificate Store
      LIST Certificate_Store -                  List All Certificates
In Specified Certificate Store
```

VIEW Certificate_Store Certificate_Name Certificate_UID - View Details Of Specified Certificate In Specified Certificate Store

No parameter - Lists Usage



DISABLE CRESTRON CLOUD

Rationale: Crestron's devices reach out to the Cloud for uptime information or other diagnostic information. This may be against a site policy.

```
ENABLEFEATURE CLOUDCLIENT OFF
```

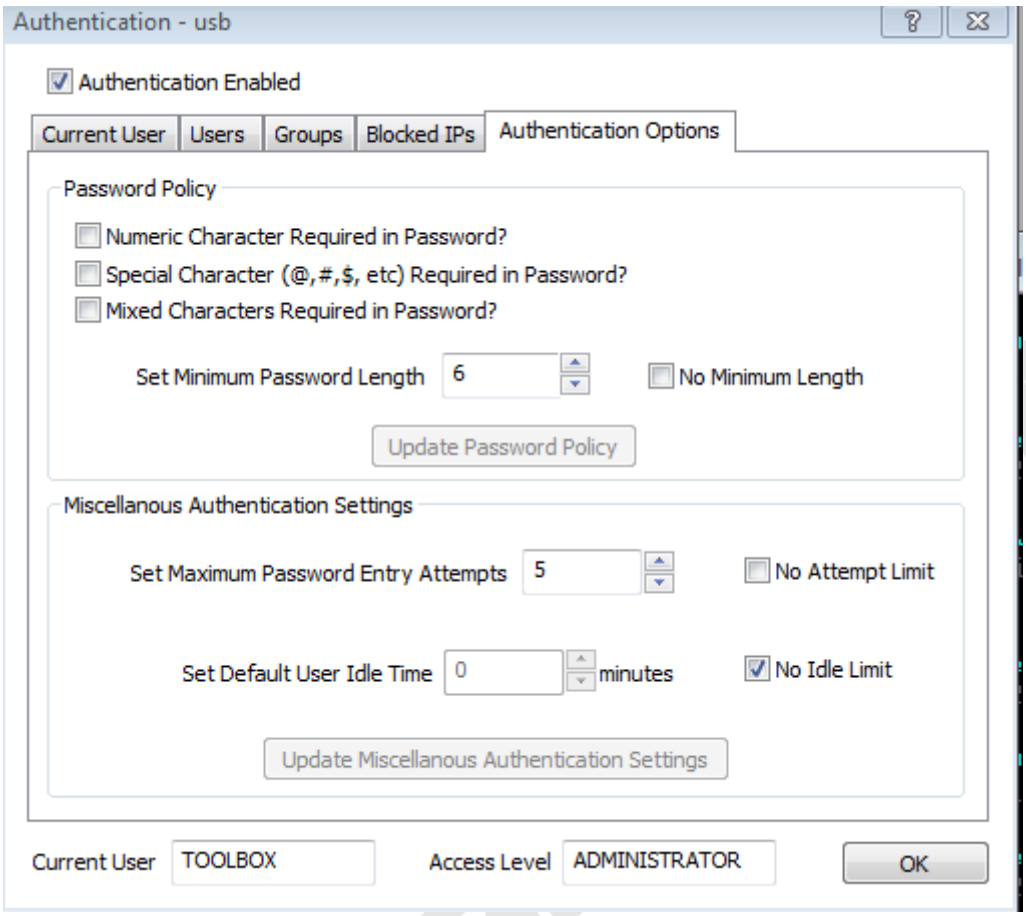
SET IDLE TIME OUT

Rationale: A user might forget to log out of a console window using the LOGOFF command.

```
PRO3>setlogoffidletime ?
SETLOGOFFIDLETIME [minutes]
```

minutes: idle minutes passed before current user is logged off (Limit 7 days). 0 means user will NOT be logged off automatically.

No parameter: display current transport setting


Authentication - usb
Authentication Enabled
Current User
Users
Groups
Blocked IPs
Authentication Options
Password Policy
Numeric Character Required in Password?
Special Character (@,#,$, etc) Required in Password?
Mixed Characters Required in Password?
Set Minimum Password Length
6
No Minimum Length
Update Password Policy
Miscellanous Authentication Settings
Set Maximum Password Entry Attempts
5
No Attempt Limit
Set Default User Idle Time
0
minutes
No Idle Limit
Update Miscellanous Authentication Settings
Current User
TOOLBOX
Access Level
ADMINISTRATOR
OK

SETUP AUDIT LOGS

Rationale: A secure system requires monitoring access.

NOTE: The system cycles through space pre-allocated for audit logs. It is the site responsibility to ensure these logs are archived on a regular basis if a complete history is required.

The Audit Log(s) can be retrieved from sftp://AuditLog or via the SSH console command below.

NOTE RECOMMENDED SETTINGS: `AUDITLOG ON ALL`

```
PRO3>auditlog ?
AUDITLogging [ON|OFF] {[ALL]|[NONE]|{[ADMIN] [PROG] [OPER] [USER]}}
```

`ON`: Enable Logging

`OFF`: Disable Logging

No parameter: Displays current setting

NOTE: Logons, logoffs, and account management are always logged

- optional, used to log commands by access level

`ADMIN`: Administrator

`PROG`: Programmer

`OPER`: Operator

`USER`: User

`ALL`: All Access Levels

`NONE`: No Command Logging

Example: `'AUDITLOGGING ON ADMIN OPER'`

```
PRO3>printauditlog ?
PRINTAUDITLOG {[ALL]}
```

`All`: Print the entire audit log

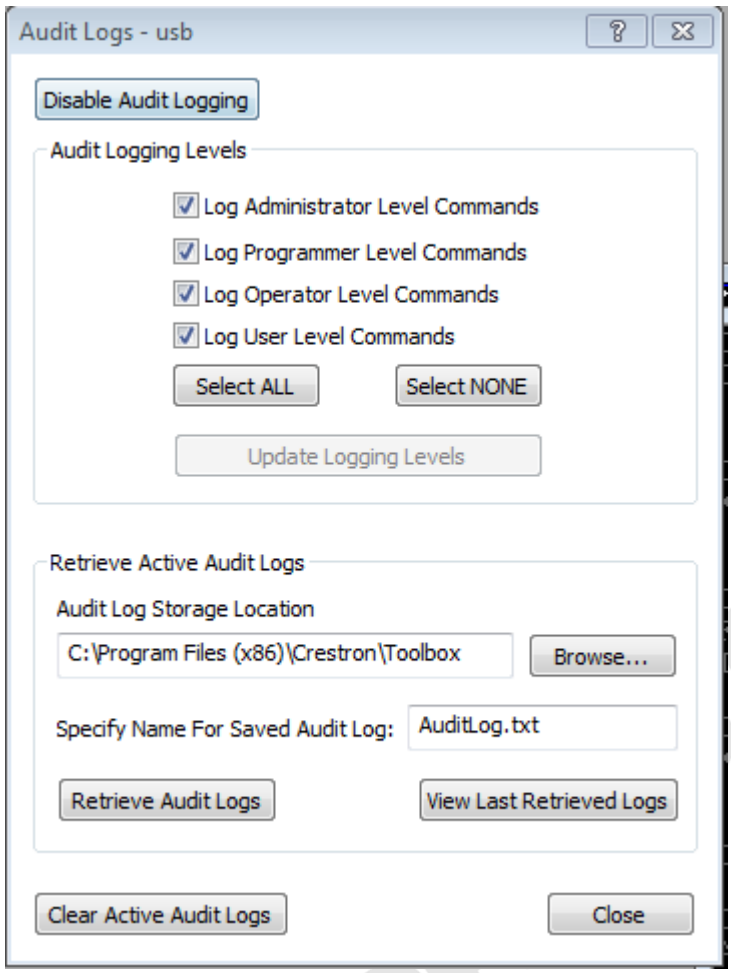
No parameter: Print the last 50 entries from the log

```
PRO3>clearauditlog ?
CLEARAUDITLOG
```

No parameter: Clears the audit log

```
PRO3>printauditlog
[12/19/2014 1:44:09 PM]: EVENT: COMMAND (DynTrans_SimplSharpPro.exe)  USER: Console Symbol         # RSLVHostname
[12/19/2014 1:49:09 PM]: EVENT: COMMAND (DynTrans_SimplSharpPro.exe)  USER: Console Symbol         # RSLVHostname
[12/19/2014 1:54:09 PM]: EVENT: COMMAND (DynTrans_SimplSharpPro.exe)  USER: Console Symbol         # RSLVHostname
[12/19/2014 1:59:09 PM]: EVENT: COMMAND (DynTrans_SimplSharpPro.exe)  USER: Console Symbol         # RSLVHostname
[12/19/2014 2:04:09 PM]: EVENT: COMMAND (DynTrans_SimplSharpPro.exe)  USER: Console Symbol         # RSLVHostname
[12/19/2014 2:09:09 PM]: EVENT: COMMAND (DynTrans_SimplSharpPro.exe)  USER: Console Symbol         # RSLVHostname
[12/19/2014 2:14:09 PM]: EVENT: COMMAND (DynTrans_SimplSharpPro.exe)  USER: Console Symbol         # RSLVHostname
[12/19/2014 2:19:09 PM]: EVENT: COMMAND (DynTrans_SimplSharpPro.exe)  USER: Console Symbol         # RSLVHostname
[12/19/2014 2:24:09 PM]: EVENT: COMMAND (DynTrans_SimplSharpPro.exe)  USER: Console Symbol         # RSLVHostname
[12/19/2014 2:27:04 PM]: EVENT: COMMAND (SHELL )  USER: admin123      # HELP
[12/19/2014 2:27:41 PM]: EVENT: COMMAND (SHELL )  USER: admin123      # WHO
[12/19/2014 2:29:09 PM]: EVENT: COMMAND (DynTrans_SimplSharpPro.exe)  USER: Console Symbol         # RSLVHostname
[12/19/2014 2:29:15 PM]: EVENT: COMMAND (SHELL )  USER: admin123      # STOPTBCLIENT
[12/19/2014 2:29:36 PM]: EVENT: COMMAND (SHELL )  USER: admin123      # SNTP
```

```
[12/19/2014 2:34:09 PM]: EVENT: COMMAND (DynTrans_SimplSharpPro.exe)  USER: Console Symbol          # RSLVHostname
[12/19/2014 2:39:09 PM]: EVENT: COMMAND (DynTrans_SimplSharpPro.exe)  USER: Console Symbol          # RSLVHostname
[12/19/2014 2:44:09 PM]: EVENT: COMMAND (DynTrans_SimplSharpPro.exe)  USER: Console Symbol          # RSLVHostname
[12/19/2014 2:49:09 PM]: EVENT: COMMAND (DynTrans_SimplSharpPro.exe)  USER: Console Symbol          # RSLVHostname
[12/19/2014 2:54:09 PM]: EVENT: COMMAND (DynTrans_SimplSharpPro.exe)  USER: Console Symbol          # RSLVHostname
[12/19/2014 2:59:09 PM]: EVENT: COMMAND (DynTrans_SimplSharpPro.exe)  USER: Console Symbol          # RSLVHostname
[12/19/2014 3:04:09 PM]: EVENT: COMMAND (DynTrans_SimplSharpPro.exe)  USER: Console Symbol          # RSLVHostname
[12/19/2014 3:09:09 PM]: EVENT: COMMAND (DynTrans_SimplSharpPro.exe)  USER: Console Symbol          # RSLVHostname
[12/19/2014 3:14:09 PM]: EVENT: COMMAND (DynTrans_SimplSharpPro.exe)  USER: Console Symbol          # RSLVHostname
[12/19/2014 3:19:09 PM]: EVENT: COMMAND (DynTrans_SimplSharpPro.exe)  USER: Console Symbol          # RSLVHostname
[12/19/2014 3:19:14 PM]: EVENT: COMMAND (SHELL )  USER: admin123      # USERUNPat
[12/19/2014 3:19:14 PM]: EVENT: LOGOFF  (SHELL )  USER: admin123      # Console Session Terminated
[12/19/2014 3:24:09 PM]: EVENT: COMMAND (DynTrans_SimplSharpPro.exe)  USER: Console Symbol          # RSLVHostname
[12/19/2014 3:27:17 PM]: EVENT: COMMAND (SHELL )  USER: admin123      # VERsion
[12/19/2014 3:27:17 PM]: EVENT: COMMAND (SHELL )  USER: admin123      # ISOLATENETworks
[12/19/2014 3:27:17 PM]: EVENT: COMMAND (SHELL )  USER: admin123      # USERPAT
[12/19/2014 3:27:26 PM]: EVENT: COMMAND (SHELL )  USER: admin123      # USERUNPat
[12/19/2014 3:27:33 PM]: EVENT: COMMAND (SHELL )  USER: admin123      # HELP
[12/19/2014 3:27:43 PM]: EVENT: COMMAND (SHELL )  USER: admin123      # SETLOGINAttempts
[12/19/2014 3:27:49 PM]: EVENT: COMMAND (SHELL )  USER: admin123      # SETLOGINAttempts
[12/19/2014 3:27:57 PM]: EVENT: COMMAND (SHELL )  USER: admin123      # SETLOCKOUTTIME
[12/19/2014 3:28:56 PM]: EVENT: COMMAND (SHELL )  USER: admin123      # SETPAsswordrule
[12/19/2014 3:29:09 PM]: EVENT: COMMAND (DynTrans_SimplSharpPro.exe)  USER: Console Symbol          # RSLVHostname
[12/19/2014 3:34:05 PM]: EVENT: COMMAND (SHELL )  USER: admin123      # CERTIFicate
[12/19/2014 3:34:09 PM]: EVENT: COMMAND (DynTrans_SimplSharpPro.exe)  USER: Console Symbol          # RSLVHostname
[12/19/2014 3:35:48 PM]: EVENT: COMMAND (SHELL )  USER: admin123      # TELNETport
[12/19/2014 3:35:51 PM]: EVENT: COMMAND (SHELL )  USER: admin123      # SNTP
[12/19/2014 3:35:54 PM]: EVENT: COMMAND (SHELL )  USER: admin123      # SNTP
[12/19/2014 3:38:01 PM]: EVENT: COMMAND (SHELL )  USER: admin123      # HELP
[12/19/2014 3:38:38 PM]: EVENT: COMMAND (SHELL )  USER: admin123      # SETLogoffidletime
[12/19/2014 3:39:09 PM]: EVENT: COMMAND (DynTrans_SimplSharpPro.exe)  USER: Console Symbol          # RSLVHostname
[12/19/2014 3:40:03 PM]: EVENT: COMMAND (SHELL )  USER: admin123      # AUDITLogging
[12/19/2014 3:40:10 PM]: EVENT: COMMAND (SHELL )  USER: admin123      # PRINTAUDITLOG
[12/19/2014 3:40:16 PM]: EVENT: COMMAND (SHELL )  USER: admin123      # CLEARerr
[12/19/2014 3:40:25 PM]: EVENT: COMMAND (SHELL )  USER: admin123      # CLEARAUDITLOG
[12/19/2014 3:40:32 PM]: EVENT: COMMAND (SHELL )  USER: admin123      # PRINTAUDITLOG
--End of Log--
```


Audit Logs - usb
Disable Audit Logging
Audit Logging Levels
Log Administrator Level Commands
Log Programmer Level Commands
Log Operator Level Commands
Log User Level Commands
Select ALL
Select NONE
Update Logging Levels
Retrieve Active Audit Logs
Audit Log Storage Location
C:\Program Files (x86)\Crestron\Toolbox
Browse...
Specify Name For Saved Audit Log:
AuditLog.txt
Retrieve Audit Logs
View Last Retrieved Logs
Clear Active Audit Logs
Close

802.1X AUTHENTICATION

For installations requiring 802.1x, here are the commands you will need. Familiarity with 802.1x is assumed by this document but for convenience the instructions for Setting up 802.1x on a Windows Server may be found later in this document.

COMMANDS NEEDED FOR 802.1X AUTHENTICATION

8021XAUthenticate Enable/Disable 802.1x Authentication

```
8021xAuthenticate [ON |OFF]
```

`ON`: Enable 802.1x Supplicant Authentication

`OFF`: Disable 802.1x Supplicant Authentication

No parameter: displays current setting

8021XDOMain Configure/View 802.1x Domain Name.

```
8021xDomainName [Domain Name]
```

`DomainName`: Update Domain Name to Domain Specified

No parameter: displays current setting

8021XMEThod Configure/View EAP Method.

```
8021xMethod [Password |Certificate |List]
```

`Password`: 802.1x Supplicant Will Use Secured Password (EAP MSCHAP V2) EAP Method

`Certificate`: 802.1x Supplicant Will Use Certificate EAP Method

`List`: 802.1x Supplicant Will display the supported EAP Methods

No parameter: displays current setting

8021XPASsword Configure 802.1x Password.

```
8021xPassword [Password]
```

`{Password}`: Update Password to One Specified

No parameter: Echo back command

8021XSENdpeapver Enable/Disable 802.1x PEAP version reporting.

```
8021xSendPeapVer [ON |OFF]
```

`ON`: enable 802.1x PEAP version number report

`OFF`: disable 802.1x PEAP version number report

No parameter: displays current setting

8021XTRUStedcas Select/List 802.1x Trusted CA Certificates.

```
8021xTrustedCAs [LIST|USE|DONTUSE] <Certificate_Name
Certificate_UID>)
```

`LIST`: List All Trusted Root Certificates

USE {Certificate Name and UID}: Add Specified Certificate To List Of Certificates Used To Validate The Server

DONTUSE {Certificate Name and UID}: Remove Specified Certificate From List Of Certificates Used To Validate The Server

No parameter: Display this help message

8021XUSERname Configure/View 802.1x User Name.

8021xUsername Password <Name>

Password: Displays current settings

Password {Name}: Update User Name To Name Specified

No parameter: Displays Help Menu

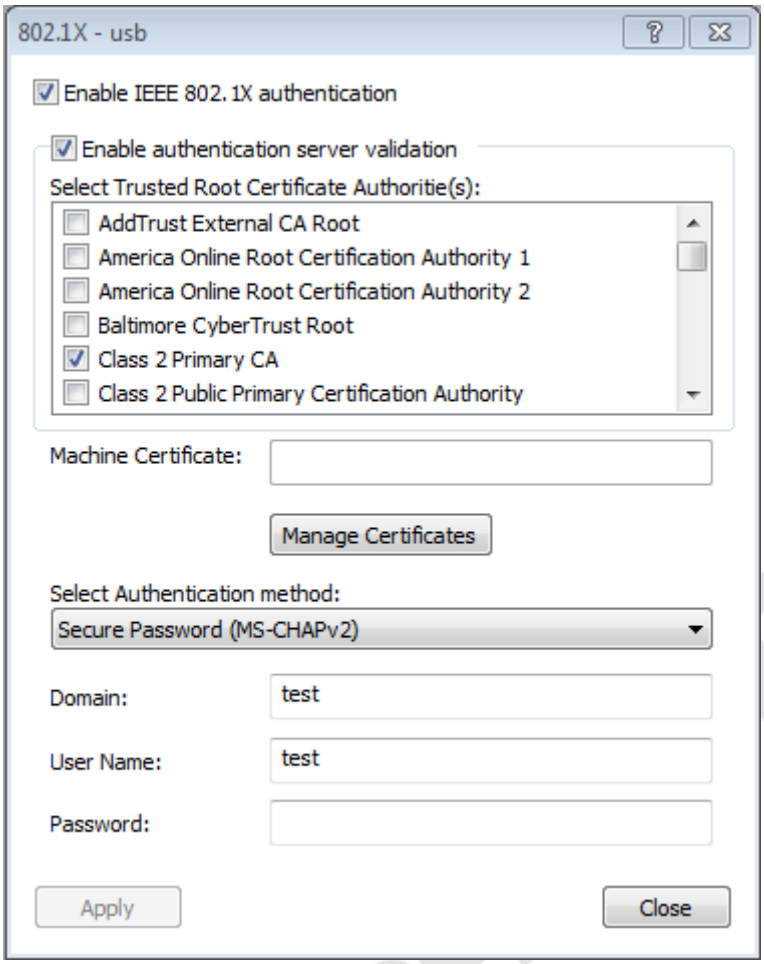
8021XVALidateserver Require Validation Of 802.1x Authentication Server's Certificate.

8021xValidateServer [ON |OFF]

ON: 802.1x Supplicant Will Validate Authentication Server's Certificate

OFF: 802.1x Supplicant Will Not Validate Authentication Server's Certificate

No parameter: displays current setting


802.1X - usb
Enable IEEE 802.1X authentication
Enable authentication server validation
Select Trusted Root Certificate Authorities(s):
AddTrust External CA Root
America Online Root Certification Authority 1
America Online Root Certification Authority 2
Baltimore CyberTrust Root
Class 2 Primary CA
Class 2 Public Primary Certification Authority
Machine Certificate:
Manage Certificates
Select Authentication method:
Secure Password (MS-CHAPv2)
Domain:
test
User Name:
test
Password:
Apply
Close

SECURITY PROTOCOLS

Details about used protocols are located here.

For management over SSH, a client capable of connecting over SSHv2 is required. The SSH client must be compliant with a FIPS 140-2 validated server.

Crestron products use one or more of the following FIPS validated libraries:

- OpenSSL FIPS Object Module v2.0 has FIPS 140-2 certificate #1747.
- OpenSSL FIPS Object Module v1.2.x has FIPS 140-2 certificate #1051.
- Windows Embedded Compact Cryptographic Primitives Library (bcrypt.dll) has FIPS 140-2 certificate #1989.
- Microsoft Windows CE and Windows Mobile Enhanced Cryptographic Provider 6.00.1937 and Microsoft Windows Embedded Compact Enhanced Cryptographic Provider 7.00.1687 has FIPS 140-2 certificate #825.

MORE ABOUT USER GROUPS

The architecture shall support multiple user groups (either locally or from Active Directory). Any user can be a member of multiple groups. Both local and Active Directory groups can be given rights, such as the following:

1. Log into console/Telnet and have access to read-only system status/setting commands.
2. Use customer web x-panel.
3. Use setup web x-panel.
4. Log in to connect to CIP/Gateway connections (such as RoomView).
5. Administrator commands are console commands that we rate as administrator. This includes commands that have to do with user accounts and changing system settings.
6. Programmer commands are console commands that we rate as programmer. This includes commands that have to do with loading programs and loading files.
7. Operator commands are console commands that we rate as operator. This includes commands that have to do with restarting programs, etc.

Out of the box, the device shall ship with the following local user groups with the associated rights.

	1	2	3	4	5	6	7	Comments
Crestron Admin	Y	Y	Y	Y	Y	Y	Y	
Crestron Programmer	Y	Y	N	Y	N	Y	Y	
Crestron Operator	Y	Y	N	Y	N	N	Y	
Crestron User	N	Y	N	N	N	N	N	
Crestron Connect	N	N	N	Y	N	N	N	

TSW-752

To harden a TSW-752, TSW-552, TSW-1052, please use the following commands.

- `AUTHENTICATION ON`
- `TELNETPORT OFF`
- `SSL NOVERIFY`
- If talking to a control system with Authentication on (in the control system), supply user/password for the control system CIP connection via `SETCSAUTHENTICATION` command.
- `SIPENABLE OFF`
- `FTPSERVER OFF`
- `ENTERSETUPSEQ DISABLE`

DIGITAL MEDIA

MATRIX SWITCHES

The following information applies to the DM-MD8x8, DM-MD16x16, DM-MD32x32.

Please execute the following commands

TELNETPORT OFF
SSL SELF
PASSWORD

Note – a rooted certificate can also be used.

SSL [OFF | SELF | CA]
where 'OFF' turns off SSL,
where 'SELF' sets SSL to use 'self-signed' certificates,
where 'CA' sets SSL to use 'CA' issued certificates,
No parameter - displays current setting

TRANSMITTER AND RECEIVER DEVICES

Transmitter and receiver devices may be controlled over the DigitalMedia link. It is not necessary to populate the LAN port. The following information applies to all DigitalMedia devices with a LAN courtesy port.

Please execute the following commands

PORTDISABLE EXTERNAL

ENABLING REMOTE ACCESS

When enabling remote access to a system, always remap external ports from the defaults. This can cut down on the number of attempts to access the system as a hacker can't simply scan well-known ports for entry and instead must scan all ports and then try and figure out what protocols they support before even attempting to login to the system.

Most home routers will allow setting a different external and internal port number. For example, this is the setup page for a well-known home router.

Single Port Forwarding

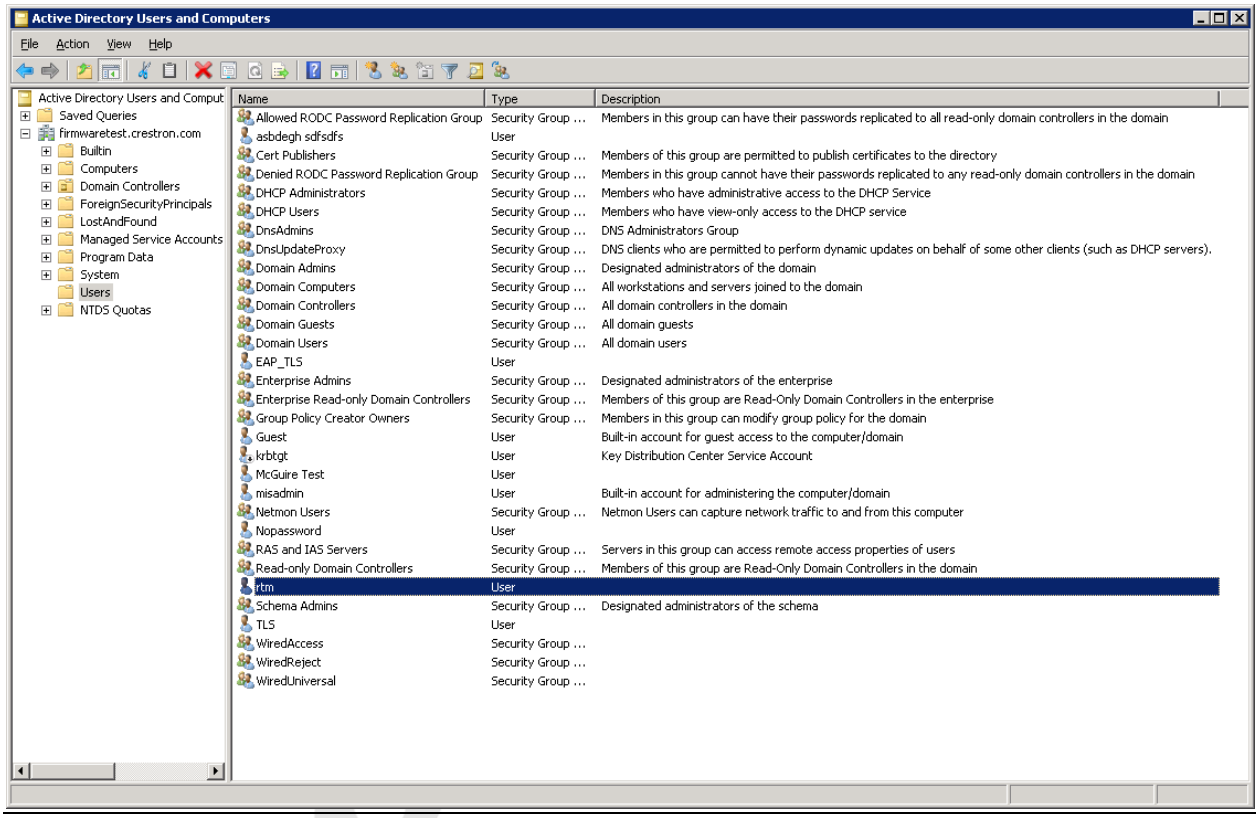
Application Name	External Port	Internal Port	Protocol	To IP Address	Enabled
None	---	---	---	192 . 168 . 194. 0	☐
None	---	---	---	192 . 168 . 194. 0	☐
None	---	---	---	192 . 168 . 194. 0	☐
None	---	---	---	192 . 168 . 194. 0	☐
None	---	---	---	192 . 168 . 194. 0	☐
CIP	9699	41796	Both	192 . 168 . 194. 99	☑
SSH	2299	22	Both	192 . 168 . 194. 99	☑
eControl	4499	443	Both	192 . 168 . 194. 99	☑
Policy File	843	843	Both	192 . 168 . 194. 99	☑

Note the exception on the policy file support. If you need XPanel Web Browser you will need to open up port 843.

SETTING UP 802.1X ON A WINDOWS SERVER

Below are the 802.1x setup instructions for Windows 2008 server.

SETTING UP ACTIVE DIRECTORY

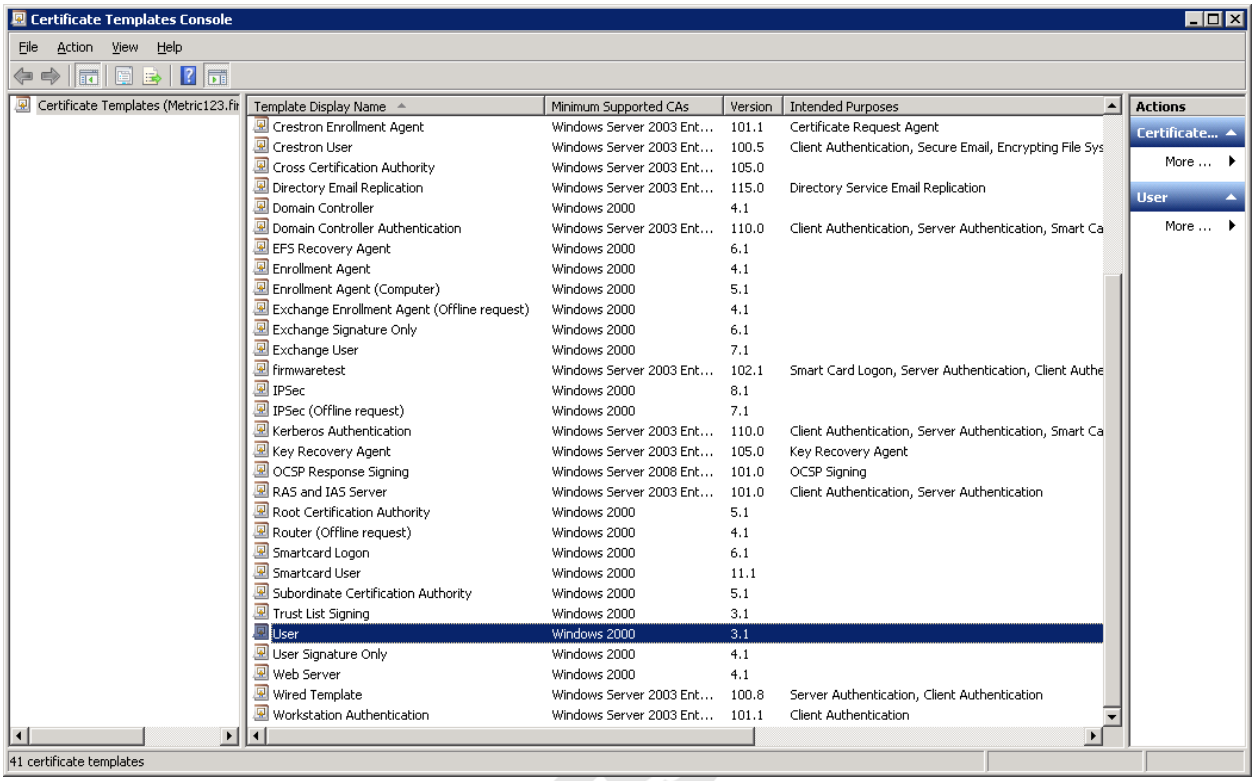


- Click View drop down -> Enable Advanced Features.
- Click Action drop down menu.
- Select New and choose User Type.
- Enter the logon name and password for the user. This will be used for the PEAP-MSCHAPv2 Authentication.
- Select New and choose Computer Type.
- Enter the hostname of the controller as the computer name. This will be used for EAP-TLS Authentication.

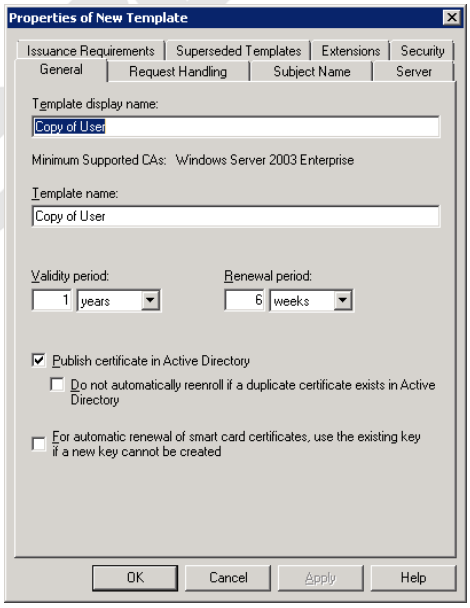
SETTING UP CERTIFICATE AUTHORITY

SETTING UP CERTIFICATE TEMPLATE

- Click Start Menu -> Administrative Tools -> Certification Authority.
- Right Click Certificate Template -> Manage.

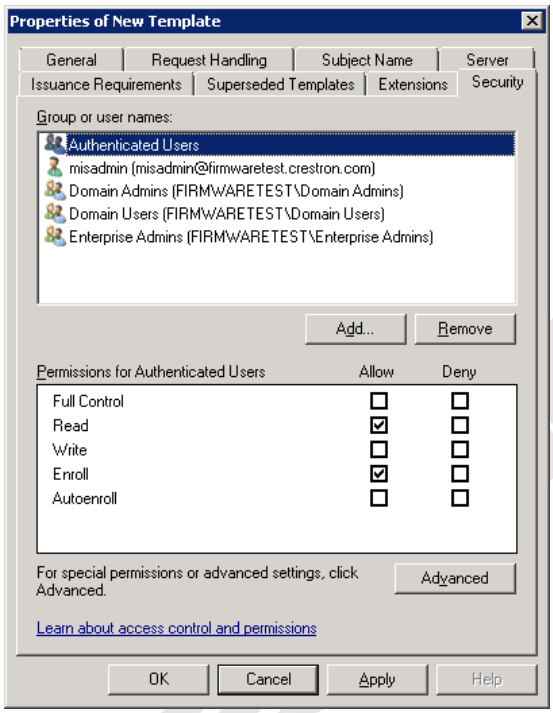


- Select User -> Right Click-> Duplicate Template -> Windows 2003 Enterprise.



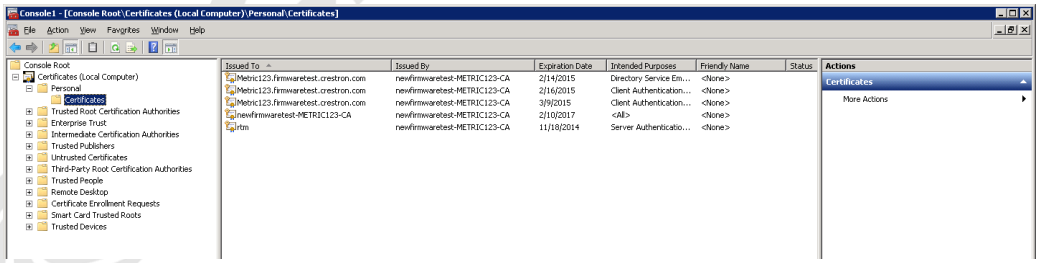
- Enter Template Name (for example, Crestron Computer)
- Choose a validity period. Choosing a 1 year validity creates certificates that have 1 year of validity.
- Under Request handling tab -> Select Allow private key to be exported.

- Under Subject Name tab -> Select supply in request.
- Under Security tab -> Enable the Enroll permission for Authenticated Users and Admin.

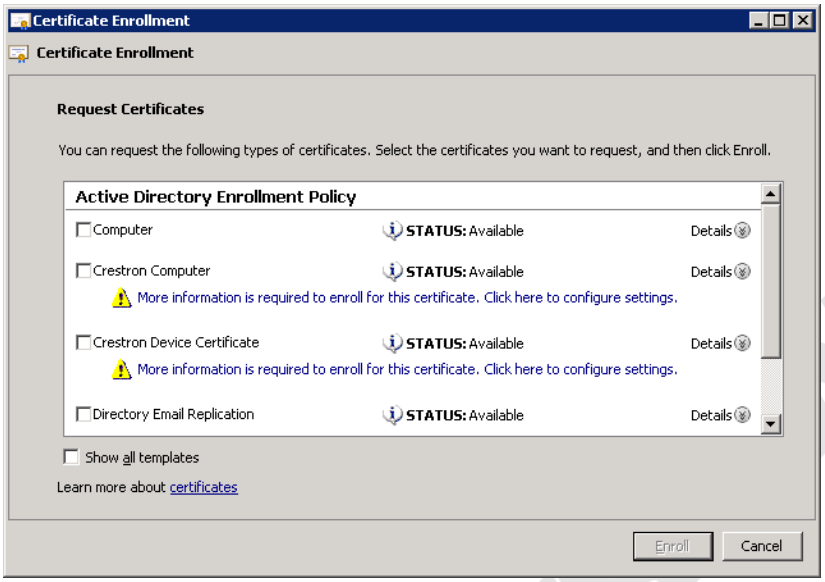


ISSUE CERTIFICATE BASED ON TEMPLATE

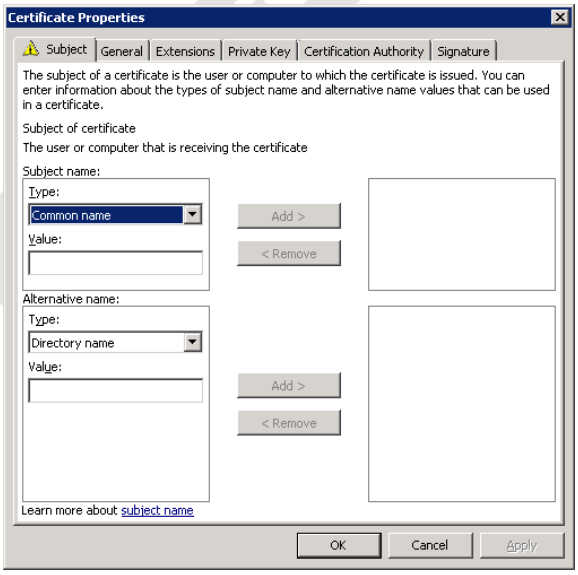
- Run\Open MMC Console.
- Under File -> Add\Remove Snap-in -> Certificates -> Add -> Choose Computer Account.



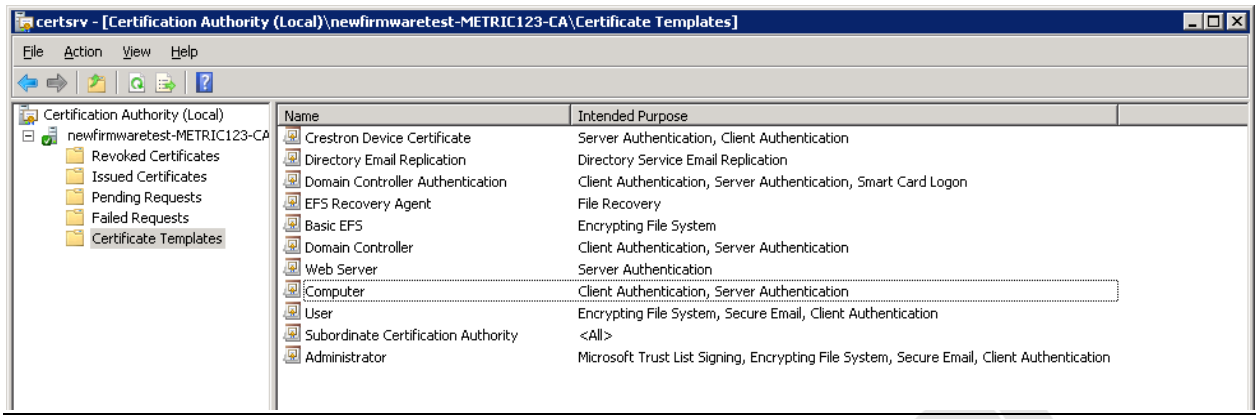
- Certificates -> Personal -> Certificates.
- Under Action -> All tasks -> Request New Certificate.
- Select Active Enrollment Policy -> Next.



- Select the template created above (for example, Crestron Computer)
- Under Subject tab -> Subject name type -> Common Name - > Value: Hostname of the Controller -> Add.
- Click Enroll. A certificate with the hostname of the controller will be created.

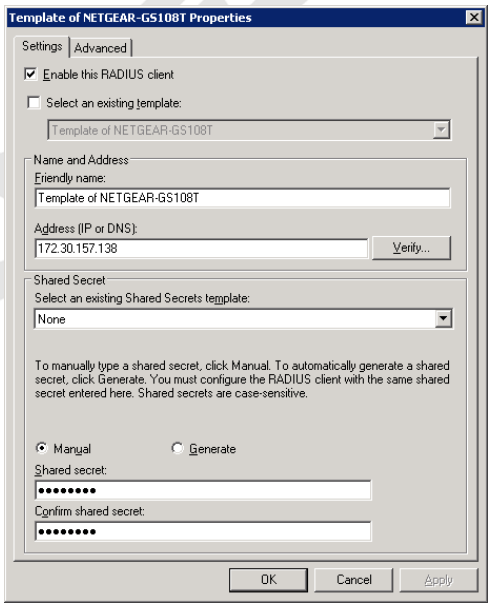


- Right click machine certificate -> All tasks -> Export
  - Export the certificate with private key. This becomes the machine certificate for the controller.
  - Export the certificate without the private key. This becomes the machine's public key for the Radius Server.

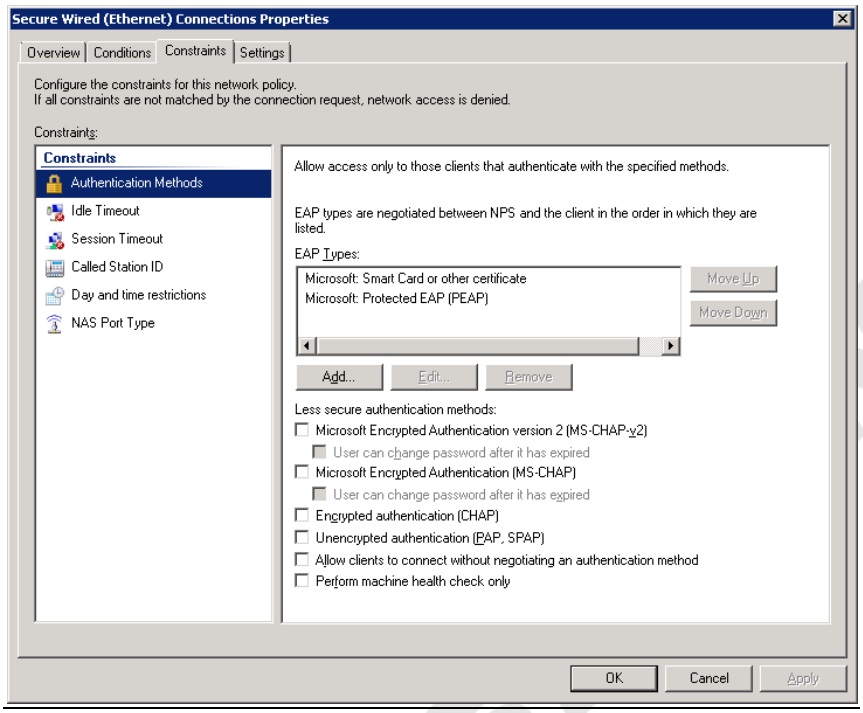


SETTING UP RADIUS SERVER

- Go to Start Menu -> Administrative Tools -> Network Policy Server.
- Select RADIUS Clients and Servers -> Right Click RADIUS Clients -> New.
- Select Enable RADIUS Client.
- In Address, enter the address of the 802.1x switch.
- In Shared Secret, enter the shared secret password while setting up the switch.



- Select Policies-> Network Policy -> Constraints Tab.
- Under Authentication Methods, do the following:
  - Add Microsoft: Smart Cards or certificates (EAP-TLS).
  - Add Microsoft: Protected EAP (PEAP - MSCHAPv2).
  - Select the certificate of the CA in the "Certificate Issued" drop down.



VERIFY SUCCESSFUL AUTHENTICATION

- Select Diagnostics -> Event Viewer -> Server Roles -> Network Policy and Access Services.
- If the authentication succeeds/fails, an event will be logged with the controller's hostname.