



DGW Firmware Security Guidelines

Mediatrix Product Line

Summary

Overview/Introduction	3
Important note about password synchronization and management	3
Default passwords and access	3
Choosing a secure password	4
Changing password	4
Securing the Web management interface	6
Securing the SNMP	7
Using the Local Firewall	8
Enabling TLS encryption	13
Other security settings	21
Linux Operating System	23
Copyright Notice	24

Overview/Introduction

This is a security best practices guide, based on M5 current knowledge of the most common use cases for Mediatrix product line.

Important note about password synchronization and management

When integrating Mediatrix products into mass management systems, it is important to keep in mind that each one may have different password policies and synchronization mechanisms.

Always review the specific requirements for each customer having a Mediatrix solution.

Default passwords and access

Mediatrix Specific Factory default Settings

Out of the box, or after a factory reset, M5 standard factory settings apply for any Mediatrix device/solution running MX firmware profiles, example:

- **4102-MX-D2000**
- **CXXX-MX-D2000**

System users (web interface and SSH access), both use the same password:

User Name	Password	Access Rights
admin	administrator	Full admin rights
public	“empty”	Full admin rights

SNMP management is enabled on UDP port 161:

Protocol	Community	Authentication	Auth. Protocol	Privacy Protocol (encryption)	Privacy Password (SNMP v3 only)
SNMP (v1, v2 and v3)	public	admin	MD5	None	administrator

Choosing a secure password

To be compatible with the password policies of the different call managers and management interfaces, you must change the password according to the following policies:

- Password must be from 8 to 20 characters
 - DES (used in SNMPv3) uses a 56-bit key, and the password needs to be 8x7-bit ASCII characters.
- The following policies are also required for systems using cracklib:
 - Should contain all the following:
 - Upper-case letters (A-Z)
 - Lower-case letters (a-z)
 - Numbers (0-9)
 - Special characters (` ~ ! @ # \$ % ^ & * () - _ = + .)
 - Must not contain the user's login ID (username), current password, or the default System password
 - Must not contain a dictionary word (or reversed word)
 - Must not be too simplistic/systematic
 - Must contain at least 5 unique characters

Changing password

Changing passwords via configuration scripts

Script lines to edit/add:

```
Aaa.Users[UserName=admin].Password = "New Password"

Aaa.Users[UserName=public].Password = "New Password"

Aaa.Users[UserName=admin].AccessRights = "Admin"

Aaa.Users[UserName=public].AccessRights = "User"

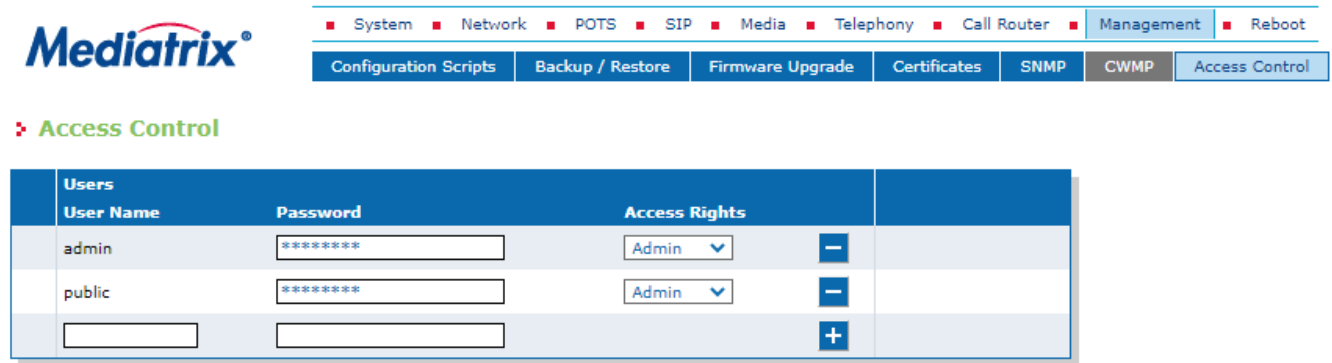
Aaa.Users[UserName=admin].LockProtectionEnable = "Enable"

Aaa.Users[UserName=public].LockProtectionEnable = "Enable"
```

Changing passwords manually on the Mediatrix web interface

The passwords can be manually changed on the Mediatrix device:

- Log in to <https://<IP of Mediatrix ATA/>> and go to the **Management/Access Control** tab.
- In the **Users** table, enter a new password for the user.
- Click **Apply**.



The screenshot shows the Mediatrix web interface. At the top, there is a navigation bar with tabs: System, Network, POTS, SIP, Media, Telephony, Call Router, Management (selected), and Reboot. Below this is a secondary navigation bar with tabs: Configuration Scripts, Backup / Restore, Firmware Upgrade, Certificates, SNMP, CWMP, and Access Control (selected). The main content area is titled "Access Control" and contains a table with the following structure:

Users			
User Name	Password	Access Rights	
admin	*****	Admin ▼	–
public	*****	Admin ▼	–
			+

For more information, refer to the Access Control Management documentation:

<https://documentation.media5corp.com/display/DGWLATEST/Access+Control+Management>

Protecting against brute-force attack attempts

Mediatrix DGW firmware has a protection against brute force login attempts (starting from DGW v48). When this protection is enabled, a user account is temporarily locked after repetitive login failures. The **Lock Protection must be set to Enable** for each user in the **Management/Access Control** tab.

The maximum number of login attempts before locking the user's account is **5** by default. After the maximum attempts, the account is disabled for **300** seconds.

These values can be configured in the Command-Line interface with the **Aaa.LoginLockedMaxRetry** and **Aaa.LoginLockedTimeout** parameters.

Securing the Web management interface

By default the web management interface is available through all network interfaces, on HTTP and HTTPS protocols.

Disabling Web service via configuration scripts

Script lines to edit/add:

```
Scm.ServicesConfig[Name=Web].StartupType = "Manual"

Scm.ServicesCommands[Name=Web].Stop
```

Disabling Web service

If the Web management is not used the best practice is to disable the service.

- Log in to <https://<IP of Mediatrix gateway/>> using the default or current credentials depending on the case.
- Go to the **System/Services** tab.
- In the **Services table**, set **Web (WEB)** to **Manual**.
- Click **Apply**.
- Click on the stop button at the right of the service .

Securing the SNMP

By default, SNMP is enabled.

Disabling SNMP service via configuration scripts

SNMP management should be disabled when deploying units on uncontrolled/open networks:

```
Scm.ServicesConfig[Name=Snmp].StartupType = "Manual"

Scm.ServicesCommands[Name=Snmp].Stop
```

Disabling SNMP service

If the SNMP is not used the best practice is to disable the service.

- Log in to <https://<IP of Mediatrix gateway/>> using the default or current credentials depending on the case.
- Go to the **System/Services** tab.
- In the **Services table**, set **Simple Network Management Protocol (SNMP)** to **Manual**.
- Click **Apply**.
- Click on the stop button at the right of the service .

Disabling SNMP protocols

It is strongly recommended to at least disable SNMP V1 and V2 since they do not use any authentication or encryption.

- Log in to <https://<IP of Mediatrix gateway/>> using the default or current credentials depending on the case.
- Go to the **Management/SNMP** tab.
- In the **SNMP Configuration table**, set the following parameters:
 - Set **Enable SNMP V1** to **Disable**
 - Set **Enable SNMP V2** to **Disable**
 - Set **Enable SNMP V3** to **Disable**
- Click **Apply**.

SNMP Protocol	
Enable SNMP V1:	Disable ▾
Enable SNMP V2:	Disable ▾
Enable SNMP V3:	Disable ▾

Using the Local Firewall

NOTES:

- Mediatrix gateways should never be connected directly to the Internet, these devices should always connect to the Internet via a properly configured firewall.
- These guidelines apply for the Mediatrix 4102, C7, G7, S7 Series, Sentinel 100, and Sentinel 400.
- **For Sentinel SBC software solution: please refer to “Linux Operating System” section.**

The Mediatrix DGW Firmware includes a local firewall. The service allows you to protect the host unit from receiving packets from unwanted or unauthorized peers. It is designed to offer basic protection only and **not** intended as a replacement for a dedicated enterprise grade firewall. **Please read and understand the following section before using the service.**

Important notes about the Local Firewall

- The local firewall only protects the Mediatrix gateway and does not protect other hosts on the network.
- It supports IPv4 only.
- The maximum number of firewall rules is 20.
- Before setting the Default Policy to Drop, always make sure at least one rule accepts incoming packets for your PC or management networks; otherwise, the communication with the Mediatrix gateway will be lost.

Deciding on a Default Policy

When configuring a firewall, the key element is the default policy, which determines what happens when traffic is not matched by any other rules.

The default policy of **Accept** means everything is allowed except a certain list of ports or IP addresses that are specifically defined (blacklist). It is generally easier to get reachable services out-of-the-box while preventing, for example, SIP scanners on port 5060.

The default policy of **Drop** means that any traffic not matched by an explicit rule will not be allowed. This is akin to a whitelist. It is the more secure approach. However, it can be more complicated to setup, especially for VoIP, because of the need to whitelist every possible RTP port range.

It is usually recommended to start with the basic **Accept** policy when installing a new system, then adopt the more restrictive approach once the whole scenario has been tested and deployed.

Enabling the Firewall and adding management IP addresses

By default, the local firewall is started automatically at boot-up, with a **Default Policy** set to **Accept**. This means that all incoming packets for established or related connections are allowed.

Before changing the policy, or adding rules to drop packets, it is essential to start by adding specific rules to allow the management IP tools full access to the device. These generally include the PC you're using to configure the unit, as well as the Broadworks DMS and the main telephony server(s).

- Go to the **Network/Local Firewall** tab.
- Leave the **Default Policy** to **Accept**.
- Click on the **+** icon to add a new rule for your PC:
 - Set **Activation** to **Enable**.
 - Set **Source Address** to the **IP address of your PC**.
 - Leave all other fields to their default values (Protocol=All, Action=Accept).
- Perform the same operation for the **Broadworks DMS**.
- Perform the same operation for each **telephony server(s)**.
- Click **Save & Apply**.

Local Firewall Configuration	
Default Policy:	Accept ▾
Blacklist Timeout:	60
Blacklist Rate Limit Timeout:	60

Local Firewall Rules											
#	Activation	Source Address	Source Port	Destination Address	Destination Port	Protocol	Blacklist enable	Action	Rate Limit Value	Rate Limit Time Period	
1	Enable ▾	Your PC IP address				All ▾	☐	Accept ▾	10	60	⬆ ⬇ ⬆ ⬇
2	Enable ▾	Broadworks IP				All ▾	☐	Accept ▾	10	60	⬆ ⬇ ⬆ ⬇
3	Enable ▾	Telephony server IP				All ▾	☐	Accept ▾			⬆ ⬇ ⬆ ⬇
+											

Save Save & Apply Cancel Edits

It is also recommended to add an additional rule in case you ever need to reconfigure the IP addresses of the unit:

- The 192.168.0.0/28 network will allow you to connect to the Lan1 default IP address with a laptop connected on ETH2/LAN using an IP in the 192.168.0.1-192.168.0.14 range.

Enable ▾	192.168.0.0/28				All ▾	☐	Accept ▾	10	60	⬆ ⬇ ⬆ ⬇
----------	----------------	--	--	--	-------	--------------------------	----------	----	----	---------

Firewall rules with Default Policy = Accept

In this example, we will show a standard set of firewall rules using the Accept Default Policy. We will assume only the network 10.0.0.0/8 must have access to the management interfaces. Also, we will restrict SIP traffic to the specific SIP trunk IP.

- First, make sure the section “Enabling the Firewall and adding management IP addresses” has been performed and make sure the PC and other management networks have rules defined and applied.
- We will add a rule to accept only traffic from the 10.0.0.0/8 network to the management ports.
- Next, we will drop all SSH, SNMP, HTTPS and HTTP packets:
 - SSH (22 TCP)
 - SNMP (161 UDP)
 - HTTP (80 TCP)
 - HTTPS (443 TCP)
 - Note that these will still be accessible from your PC since the first matching rule is always executed first.
- Then, we add rules to allow the SIP trunk IP to access ports 5060 and 5061 in both UDP and TCP (TLS uses TCP as well) and drop all other addresses.

Local Firewall Configuration	
Default Policy:	Accept
Blacklist Timeout:	60
Blacklist Rate Limit Timeout:	60

Local Firewall Rules											
#	Activation	Source Address	Source Port	Destination Address	Destination Port	Protocol	Blacklist enable	Action	Rate Limit Value	Rate Limit Time Period	
1	Enable	Your PC IP address				All	☐	Accept	10	60	⬆ ⬇ ⬆ ⬇
2	Enable	10.0.0.8/8				All	☐	Accept	10	60	⬆ ⬇ ⬆ ⬇
3	Enable	192.168.0.10/28				All	☐	Accept	10	60	⬆ ⬇ ⬆ ⬇
4	Enable				22	TCP	☐	Drop	10	60	⬆ ⬇ ⬆ ⬇
5	Enable				161	UDP	☐	Drop	10	60	⬆ ⬇ ⬆ ⬇
6	Enable				80	TCP	☐	Drop	10	60	⬆ ⬇ ⬆ ⬇
7	Enable				443	TCP	☐	Drop	10	60	⬆ ⬇ ⬆ ⬇
8	Enable	Telephony server IP			5060-5061	UDP	☐	Accept	10	60	⬆ ⬇ ⬆ ⬇
9	Enable	Telephony server IP			5060-5061	TCP	☐	Accept	10	60	⬆ ⬇ ⬆ ⬇
10	Enable				5060-5061	UDP	☐	Drop	10	60	⬆ ⬇ ⬆ ⬇
11	Enable				5060-5061	TCP	☐	Drop	10	60	⬆ ⬇ ⬆ ⬇
											+

Save Save & Apply Cancel Edits

Firewall rules with Default Policy = Drop

In this example, we will show the same configuration as the previous section but using the Drop Default Policy. Again, we will assume only the network 10.0.0.0/8 needs to have access to the management interfaces and restrict SIP traffic to the specific SIP trunk IP.

- First, make sure the section “Enabling the Firewall and adding management IP addresses” has been performed and make sure the PC and other management networks have rules defined and applied.
- Then, we can set the policy to **Drop**.
- Since the policy is to drop everything by default, rules for SSH/SNMP/HTTPS/HTTP ports are not required.
- We will add a rule to accept only traffic from the 10.0.0.0/8 network to the management ports.
- Then, we add rules to allow the SIP trunk IP to access ports 5060 and 5061 in both UDP and TCP (TLS uses TCP as well) and drop all other addresses.
- Finally, we add three rules to deal with the RTP traffic:
 - The range of ports used for RTP media are 5004-6092 and the range of ports for T.38 is 6004-6244. Since these ports overlap with the SIP ports, we will split into ranges 5004-5059 and 5062-6244.

Local Firewall Configuration		
Default Policy:	Drop	
Blacklist Timeout:	60	
Blacklist Rate Limit Timeout:	60	

Local Firewall Rules											
#	Activation	Source Address	Source Port	Destination Address	Destination Port	Protocol	Blacklist enable	Action	Rate Limit Value	Rate Limit Time Period	
1	Enable ▼	172.16.10.1				All ▼	☐	Accept ▼	10	60	⬆️ ⬇️ ➕ ➡️
2	Enable ▼	192.168.0.10/28				All ▼	☐	Accept ▼	10	60	⬆️ ⬇️ ➕ ➡️
3	Enable ▼	10.0.0.8/8			22	TCP ▼	☐	Accept ▼	10	60	⬆️ ⬇️ ➕ ➡️
4	Enable ▼	10.0.0.8/8			161	UDP ▼	☐	Accept ▼	10	60	⬆️ ⬇️ ➕ ➡️
5	Enable ▼	10.0.0.8/8			80	TCP ▼	☐	Accept ▼	10	60	⬆️ ⬇️ ➕ ➡️
6	Enable ▼	10.0.0.8/8			443	TCP ▼	☐	Accept ▼	10	60	⬆️ ⬇️ ➕ ➡️
7	Enable ▼	25.26.25.32			5060-5061	UDP ▼	☐	Accept ▼	10	60	⬆️ ⬇️ ➕ ➡️
8	Enable ▼	25.26.25.32			5060-5061	TCP ▼	☐	Accept ▼	10	60	⬆️ ⬇️ ➕ ➡️
9	Enable ▼				5004-5059	UDP ▼	☐	Accept ▼	10	60	⬆️ ⬇️ ➕ ➡️
10	Enable ▼				5062-6244	UDP ▼	☐	Accept ▼	10	60	⬆️ ⬇️ ➕ ➡️
+											

Save Save & Apply Cancel Edits

Ports used by the Mediatrix gateways

Listening ports		
Connection Type	Default Port(s)	Transport Protocol
SSH	22	TCP
HTTP	80	TCP
SNMP (Management)	161	UDP
HTTPS	443	TCP
SIP	5060	UDP / TCP
SIP/TLS	5061	TCP (TLS)
SIP (Alternate ports)	5062-5069	UDP / TCP / TLS
RTP/SRTP	5004-6092	UDP
T.38	6004-6244	UDP

Outbound ports		
Connection Type	Default Port(s)	Transport Protocol
FTP	21	TCP
DNS	53	UDP
DHCP	68	UDP
TFTP	69	UDP
SNTP	123	UDP
SNMP Trap	162	UDP
Syslog	514	UDP
Radius default port for authentication	1812	TCP
Radius default port for accounting	1813	TCP
Debug Signaling Log Host	6000	UDP
Persistent TLS or endpoint gateway	16000-16028	UDP / TCP / TLS

Enabling TLS encryption

By default the TLS is disabled, and a host self-signed certificate is required. It is strongly suggested to configure the certificate to allow a dual authentication. The same host certificate can be assigned for Web and SIP.

Note: A Trusted CA can be used in place of this as described in *Importing a Trusted CA*.

Using CA Certificates

Digital certificates can be used, which are a collection of data used to verify the identity of individuals, computers, and other entities on a network.

Certificates contain:

- the certificate's name
- the issuer and issued to names
- the validity period (the certificate is not valid before or after this period)
- the use of certificates such as:
 - TlsClient: The certificate identifies a TLS client. A host authenticated by this kind of certificate can act as a client in a SIP over TLS connection when mutual authentication is required by the server.
 - TlsServer: The certificate identifies a TLS server. A host authenticated by this kind of certificate can serve files or web pages using the HTTPS protocol or can act as a server in a SIP over TLS connection.
- whether or not the certificate is owned by a Certification Authority (CA)

Although certificates could come factory-installed new ones can also be added. Since certificates have a validity period (start date and expiry date), the use of NTP (Network Time Protocol) is mandatory when using the security features.

Two types of certificates can be used:

- Host Certificates: used to certify the unit (e.g.: a web server with HTTPS requires a host certificate).
- Others: Any other certificate including trusted CA certificates used to certify peers (e.g.: a SIP server with TLS).

To enable a TLS connection, no CA certificate needs to be installed if the respective parameters for each secure service (e.g. SIP, Conf, Cwmp, etc) has the NoValidation value. If the value is different than NoValidation, then at least one CA certificate needs to be installed. This certificate must be uploaded to the unit. The Mediatrix gateway checks the server identity by validating the host name used to contact it against the information found in the server's certificate. If the validation fails, the unit refuses the secure connection. For the SIP over TLS service, we have four (4) levels of validation: HostName, trustedCertificate, DNSSRV, and NoValidation (for a complete description of the validation levels, refer to the Help of the DGW Web interface under SIP/Interop). The way that the remote peer is evaluated for secure connection differs for each level.

Remember that the unit must be correctly configured with an SNTP server because the TLS server certificate is also validated in terms of time (certificate validation/expiration date, etc.).

For example, in a setup for two Mediatrix gateways with no SIP proxy in the middle. At least one of the units will require a Host certificate. If only one unit has a Host certificate, the calls will be allowed in only one direction (Unit 1 calls Unit 2). For bi-directional calls, both units would require a Host certificate. By default, it is not possible to upload a Host certificate without first clicking on Activate unsecure certificate transfer. This is because the certificate upload will be done in clear text, which means the private key will be susceptible to interception.

Certificates are used to secure the following connections:

- SIP
- Configuration Web pages
- File transfers (scripts, firmware, etc.) with HTTPS
- Configuration using TR-069
- Wired Ethernet Authentication with EAP (802.1x).

Host Certificates

To enable HTTPS or SIP with TLS, the unit requires a Public key certificate. This certificate is not present in the factory configuration.

To validate that a Host Certificate is present:

- Log in to <https://<IP of Mediatrix gateway/>> and go to the **Management/Certificates** tab.
- Make sure there is a certificate present and is within the Valid From and Valid To dates.
- In the Host Certificate Associations, make sure each required service is associated with a certificate.

Host Certificates						
File Name	Issued To	Issued By	Valid From	Valid To	Usage	
Other Certificates						
File Name	Issued To	Issued By	Valid From	Valid To	Usage	CA
Cert_MxDefault001.der	Media5 Corporation - Mediatrix Primary CA	Media5 Corporation - Mediatrix Primary CA	2015-03-06 15:06:40	2065-03-06 15:06:40	TlsClient, TlsServer	Yes 

For more information on host certificates, visit:

<https://documentation.media5corp.com/display/DGWLATEST/Creating+a+Media5+Device+Host+Certificate+with+OpenSSL>

Importing a Trusted CA

To import a Trusted CA into the unit:

- Go to **Management/Certificates**.
- Click **Activate unsecure certificate transfer** if needed.
- In the Certificate Import Through Web Browser table, from the Type selection list, select Other.
- Click **Browse** and select your certificate.
- Click **Import**.
- Click **Apply**.
- Click **restart required services** located at the top of the page.

Host Certificates									
File Name	Issued To	Issued By	Valid From	Valid To	Usage				
Other Certificates									
File Name	Issued To	Issued By	Valid From	Valid To	Usage	CA			
Cert_MxDefault001.der	Media5 Corporation - Mediatrix Primary CA	Media5 Corporation - Mediatrix Primary CA	2015-03-06 15:06:40	2065-03-06 15:06:40	TlsClient, TlsServer	Yes ☐			
Host Certificate Associations									
File Name	SIP	Web	EAP	Conf	Fpu	File	Cert	Nlm	CWMP
Certificate Authorities									
File Name	Override the OCSP URL for issued Certificates								
Cert_MxDefault001.der									
Certificate Import Through Web Browser									
Type	Path								
Host v	Choose File VeriSignClass3PublicPrimaryCertification-G5.crt Import								
Apply									

Enabling TLS Transport for SIP

Important:

- Mediatrix gateways do not support a mix of both TLS and non-TLS links. Once TLS is **enabled**, all configured gateways will use TLS, and all other protocols will be disabled.
- Your telephony server must be also configured in TLS.

To enable TLS:

- Navigate to the **SIP/Transport** tab.
- In the **Protocol Configuration** table, set **TLS** to **Enable**.
- Click **Apply**.
- You will need to restart the required services.

Setting the SIP to use Secure RTP

Important: the settings must also match the configuration of your telephony server(s). To enable or force Secure RTP (SRTP):

- Go to the **Media/Security** tab.
- To set the security for all ports on the system, leave **Select Endpoint** to **Default**, or choose a specific endpoint you want to configure in the drop-down menu.
- Under the **RTP** section, set Mode to Secure.
- Set the other parameters based on your desired configuration.
- Click **Apply**.

Security	
RTP	
Mode:	Secure ▼
Key Management Protocol:	SDES ▼
Encryption:	AES_CM_128 ▼
T.38	
Allow unsecure T.38 with secure RTP:	No ▼

Apply

Forcing the use of HTTPS

By default, the web management interface is accessible in HTTP mode (port 80), and HTTPS (port 443) if a certificate is present.

To force the use of HTTPS, you will need to use the Command Line Interface (CLI), either through SSH or via the **Inline Script** interface (recommended).

- Log in to https://<IP of Mediatrix gateway/
- Navigate to the **Management/Configuration Scripts/Execute** tab.
- Copy-paste the following command:
 - Web.HttpMode=Secure
- Click **Execute**.

❖ Configuration Scripts

Execute

Export

Scripts Status Execute	
Current State:	Idle
Last Result:	None
Last Successful:	

Execute Inline Script

Web.HttpMode=Secure

(Clear Script)

Execute

Disabling TLS 1.0, 1.1 and insecure cipher suites

Since the Mediatrix gateways are designed to be integrated in various environments that may include legacy systems, the factory defaults are set for maximum compatibility settings:

- The unit always will always advertise the maximum TLS version it supports, TLS 1.2, but will accept connections using TLS 1.1 or 1.0 if the peer does not support 1.2.
- The negotiated ciphers will always include the secure RSA with AES-CBC-SHA modes, but the unit will also accept the weak DES-CBC3-SHA and RC4 128 if the peer **only** supports those.

The NIST and PCI DSS standards require use of TLS 1.2 and secure ciphers.

To force TLS 1.2 and the higher CS3 cipher suite, you will need to use the Command Line Interface (CLI), either through SSH or via the **Inline Script** interface (recommended).

- Log in to https://<IP of Mediatrix gateway/
- Navigate to the **Management/Configuration Scripts/Execute** tab.
- Copy-paste the following commands:

```
Web.HttpsCipherSuite=CS3
Web.TlsVersion=TLSv1_2
SipEp.TransportTlsCipherSuite=CS3
```

- Click **Execute**.

This will disable TLS 1.0, TLS 1.1 and all ciphers but the most secure ones, for the HTTPS and SIP services. Please refer to the following sections for more information on TLS versions and Cipher suites.

TLS versions

The following TLS settings are available:

- TLSv1: Advertise TLS 1.2, but allow TLS versions 1 and up (default)
- TLSv1_1: Advertise TLS 1.2, but allow TLS versions 1.1 and up.
- TLSv1_2: Allow TLS versions 1.2 and up.
- TLSv1_3: Allow TLS version 1.3 only.

The device will always send its highest supported TLS version in the ClientHello message. The server will select the highest supported TLS version it supports from the ClientHello message. The device will then validate that the selected version is allowed. If the version is not allowed, the device will close the connection.

The TLS version is configurable by service by the following CLI commands:

```
Cert.TransferHttpsTlsVersion      =      "TLSv1_2"
Conf.ScriptsTransferTlsVersion    =      "TLSv1_2"
Conf.ImageTransferTlsVersion      =      "TLSv1_2"
Cwmp.TransportHttpsTlsVersion     =      "TLSv1_2"
File.TransferHttpsTlsVersion      =      "TLSv1_2"
Fpu.MfpTransferTlsVersion         =      "TLSv1_2"
Nlm.PcCaptureTransferTlsVersion   =      "TLSv1_2"
SipEp.TransportTlsVersion         =      "TLSv1_2"
Web.TlsVersion = "TLSv1_2"
```

Cipher Suites

The following Cipher Suites are available:

- CS1 (**default**): most compatible set of ciphers, but contains weak DES and RC4
- CS2: contains additional Diffie-Hellman Ephemeral ciphers, does not contain insecure RC4, but still has weak DES.
- CS3: contains only the most secure ciphers, including the recommended TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384.

The Cipher suite is configurable by service by the following CLI commands:

```
Cert.TransferHttpsCipherSuite      =      "CS3"
Conf.ScriptsTransferCipherSuite    =      "CS3"
Conf.ImageTransferCipherSuite      =      "CS3"
Cwmp.TransportHttpsCipherSuite     =      "CS3"
File.TransferHttpsCipherSuite      =      "CS3"
Fpu.MfpTransferCipherSuite         =      "CS3"
Nlm.PcCaptureTransferCipherSuite   =      "CS3"
SipEp.TransportTlsCipherSuite      =      "CS3"
Web.HttpsCipherSuite = "CS3"
```

Ciphers included in CS1

- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA

- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_RC4_128_MD5

Ciphers included in CS2

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA

Ciphers included in CS3

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256

Additional information

For more information on the different ciphers, please refer to the IANA assignment of TLS parameters web site:
<https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml>

There are also some interesting websites to get more information on TLS ciphers, such as:

- <https://csrc.nist.gov/Publications>
- <https://www.pcisecuritystandards.org/>
- <https://ciphersuite.info/>
- <https://www.openssl.org/docs/>
- https://owasp.org/www-project-cheat-sheets/cheatsheets/TLS_Cipher_String_Cheat_Sheet

Configuring SSH

By default, SSH is enabled on port 22, with the Standard Security Level. To change the SSH settings:

- Navigate to the **Management/Misc** tab.
- In the **CLI configuration** table you can change:
 - SSH Enable or Disable
 - SSH port
 - SSH Security Level (see below).

The **Standard** security level allows a good compromise between security and interoperability. The weakest encryption algorithms (CBC and 3DES) are excluded. The following are accepted:

- cipher: aes256-ctr, aes128-ctr
- mac: hmac-sha1, hmac-sha2-256
- key exchange: diffie-hellman-group14-sha1, diffie-hellman-group14-sha256, ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, curve25519-sha256@libssh.org

The **Most Secure** security level allows only the highest algorithms and may not work with some SSH clients:

- cipher: aes256-ctr
- mac: hmac-sha2-256
- key exchange: ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, curve25519-sha256@libssh.org

The **Permissive** security level allows all algorithms and should only be used for compatibility with old SSH clients:

- cipher: aes256-ctr, aes256-cbc, aes128-ctr, aes128-cbc, 3des-ctr, 3des-cbc
- mac: hmac-sha1, hmac-sha2-256
- key exchange: diffie-hellman-group1-sha1, diffie-hellman-group14-sha1, diffie-hellman-group14-sha256, ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, curve25519-sha256

Other security settings

Associating the Network Interface to the System Management Services

If you do not use the local firewall and want to restrict the management ports (SNMP, SSH, HTTP/HTTPS) to a specific network interface:

- Navigate to the **Management/Misc** tab.
- From the **Network Interface** selection list, select the Network Interface you wish to bind to the system management services to.
 - The internal network is **Lan1**.
 - The wan is always **Uplink**.
- Click **Apply**.

Stopping or Disabling Services

If you want to stop or disable some of the management services, for example CWMP, Web, CLI or SNMP):

- Navigate to the **System/Services** tab.
- In the **User Service** table, click  next to the service you want to stop, and set the **Startup Type** to

1 **Manual** to prevent them from starting at bootup.

- Click **Apply**.

2 Important notes:

- If you disable both Web and CLI, you will not be able to configure your unit unless you perform a factory reset.

Configuring 802.1x Authentication

To enable 802.1x authentication:

- Navigate to the **Network/Interfaces** tab and locate the In the **Ethernet Link Configuration** table.
- From the **802.1x Authentication** select **Enable** for each Ethernet link requiring 802.1x Authentication.
- Enter the **EAP username** used to authenticate each Ethernet link interfaces during the IEEE 802.1x EAPTLS authentication process..
- From the **EAP Certificate Validation** field, choose the IEEE 802.1x level of validation used by the device to authenticate the IEEE 802.1x EAPTLS peer's certificate.
- In the **EAP 802.1x Configuration** table, select the IEEE 802.1x version.
- Click **Apply**.

Disabling Partial Reset

To disable the Partial Reset function of the unit, you will need to use the Command Line Interface (CLI), either through SSH or via the **Inline Script** interface (recommended).

- Log in to `https://<IP of Mediatrix gateway/`
- Navigate to the **Management/Configuration Scripts/Execute** tab.
- Copy-paste the following command:
 - `Hardware.ResetButtonManagement="DisablePartialReset"`
- Click **Execute**.

Disabling DHCP Server Download

To ensure that a compromised DHCP server could not be used to send a configuration file to the unit:

- Navigate to the **Management/Configuration Scripts** tab.
- In the **Automatic Script Execution** table, set **Allow DHCP to Trigger Scripts Execution** to **Disable**.
- Click **Apply**.

Linux Operating System

NOTE: M5 may not support an operating system for various reasons, including discontinued support from the software vendor, lack of availability with certain products, or other reasons.

Supported Linux Distributions

- Rocky Linux 9
- Ubuntu 24.04 LTS

M5 uses and recommends these two distributions, both feature a stable (non-rolling) release and have an official long-term support, plus and Extended Security Maintenance that goes beyond 2030.

Specific Linux distribution best practices must be followed.

Linux OS support and general information

- M5 supplies reference guides to help Ubuntu users to handle specific use cases.
- Ubuntu support sites:
 - www.ubuntu.com
 - askubuntu.com/
 - www.canonical.com
- Rocky Linux support sites:
 - rockylinux.org/support/
 - wiki.rockylinux.org/rocky/support/

Copyright Notice

Copyright © 2026 M5 Technologies.

This document contains information that is proprietary to M5 Technologies.

M5 Technologies reserves all rights to this document as well as to the Intellectual Property of the document and the technology and know-how that it includes and represents.

This publication cannot be reproduced, neither in whole nor in part, in any form whatsoever, without written prior approval by M5 Technologies.

M5 Technologies reserves the right to revise this publication and make changes at any time and without the obligation to notify any person and/or entity of such revisions and/or changes.



130, rue Sauvé
Sherbrooke (Québec)
J1L 0A7 Canada
m5technologies.com