domotz

Domotz Pro Security Standards

Security is our number one concern for any feature we implement.

Domotz Pro Security Principles

Domotz has adopted administrative, physical, and technical industry-standards (including encryption, firewalls and SSL) to safeguard the security of our services and to protect the confidentiality of personally identifiable information. When designing and developing our solution we adopted the Principle of Least Privilege.

Moreover, since the early phases of development we have engaged independent third party companies to perform continuous security assessments and penetration testing and we continue to do so on a recurring basis. On a practical level, your data in the Domotz cloud is as safe as other mainstream cloud service, such us iCloud or Dropbox. We built our cloud solution on top of the best and most common practices with regard to security: as compared to other competitors in similar markets, we believe that we have placed more emphasis on security aspects.

Furthermore, security will ultimately rely on the strength of your password, hence the reason we provide hints to enforce minimum standards during account creation, and the possibility to configure two-factor authentication to access your data. We have also introduced reporting and logging for all the actions performed in your monitored networks (power control of devices, remote connections, SNMP readings, etc).

Domotz is also adapting all the internal processes to the recommendations and best practices provided within CIS 20 (Center for Internet Security - top 20 key actions).

Just to go a little bit further in details for each of possible security items:

Cloud Infrastructure

The Domotz Pro solution relies on very strict perimeter security policies. E.g. only the required standard communication ports are open to the public, while we use a different communication channel for the management. We have implemented multiple levels of firewalls keeping the front-end servers (with no-data) completely segregated from the back-end servers (managing customer data). To protect systems and data in the Domotz cloud, we adopt the "Defense in Depth" principle, which focuses on implementing several layers of security to guard against cyber threats or, in the unfortunate case of a cyber compromise, to quickly detect and mitigate its effects.

Therefore, we have got an automatic monitoring system which alerts the Domotz IT department if any strange behavior or anomalies (such as an intrusion) happens on our systems.

Domotz IT and Operation teams are subject to very stringent policies to access cloud servers, which can be accessed only via multiple levels of security steps (multi-factor authentication): VPN, RSA key and personal key/authentication.

Moreover, we have engaged external and independent third-party companies to perform continuous security assessments and penetration testing in order to guarantee the highest level of security for our cloud solution.

On a periodical basis (at least once every three months), the security committee performs a vulnerability assessment with the aim of producing a report with possible vulnerabilities.

Internal Vulnerability Assessment is based on:

- *discovery of assets*
- *automatic scans*
- *infrastructure changes review*

Finally, on a periodical basis (at least once per year), Domotz engage Cyber Security experts to perform external penetration tests on the Domotz architecture, with the aim of producing a report with possible external vulnerabilities.

External Penetration Tests are based on:

- *discovery of public available end-points*
- *manual scans of public available end-points*
- *automatic scans for known vulnerabilities*
- *TLS versions and cypher security assessments on end-points*

Account Password Management

The standard creation of an account is based on a common practice: during the creation of an account, we do not allow the user to insert short passwords, and we also provide a ranking of the strength of the password chosen, though the user is free to use a weak one.

Passwords are never sent over emails, and you can't change your account password if you do not have access to your email inbox. As a matter of fact, if you forget the password, Domotz sends a token link to your email box to change the password (we don't send you the new one directly). And you will also receive an email as soon as you change the password (so that you can spot if somebody else has changed your password).

Under no circumstances do we store your password in clear text. All the user passwords are encrypted with the highest security standards (SHA2-512).

Note: your Domotz Agent, installed on your premises on your device, (either our Domotz Box, or your private device) connects to our cloud with a different credential set (see below). So you will not even find your main password on the device.

Access to the Mobile App and online Portal can be restricted by enabling an extra layer of security to your account: two-factor authentication (2FA). Domotz users can turn on 2FA to further protect the access to their account.

Client Communication with Domotz Cloud

All communications between the Domotz App (either the Mobile App or Portal-WebApp) are established over a secure HTTPS channel (HyperText Transfer Protocol over Secure Socket Layer). As you can see from your Web Browser when connecting to the Domotz Portal or WebApp, there is a Green Lock near the URL, which means that the connection is certified to be secure.

This means that the entire communication between the Domotz App and the Cloud is over a secure channel (encrypted). Your account password is only transmitted over this secure channel to monitor and act on your network (or your client's networks).

You are the only user that can interact with your network, unless you "Invite a guest" to manage that network. You are always entitled to revoke this invitation anytime you want, so that the invited guest cannot act any more on your monitored network. Only the owner of a specific agent (network) can invite or revoke guests on his network.

Agent Communication with Domotz Cloud

All the commands to the Agent (e.g. switch on/off power outlets, control of PoE ports, etc) are sent over a secure channel (AMQPS - Advanced Message Queuing Protocol over Secure Socket Layer). Each agent/network has its own private channel, and this channel can only be accessed by that specific agent (the user/password is created at the moment of the Agent configuration, and it is only stored on your Domotz Agent device - e.g. Domotz Box, your Server, Raspberry Pi or NAS).

As said before for the Client Communication channel, we do not store the Agent password in clear text on our cloud.

Sensible information from the Agent to the Cloud are also sent over HTTPS channel, again with the same Agent credentials.

Finally, the Domotz solution does not increase the possible attack surface of the Network, since all the communications are established from within the Network toward the cloud (outgoing connections only). It creates an encrypted and temporary overlay network from within the Local Network to the Domotz Cloud. Therefore, no additional ports should be opened to the outside WAN.

Remote Connect functionality

When clicking the direct Remote Connection (it is either HTTP or HTTPS, SSH or Telnet, RDP), Domotz establishes a secure channel (Encrypted Overlay Network) between your network, our cloud and an HTTPS channel between the App (either Mobile App or WebApp). The entire communication from the App to the Agent is encrypted, such that nobody can sniff the content of it. Of course, the communication between the Agent and the end-device (e.g. a WebCam), if it is over a non-secure channel (e.g. http), is not encrypted, but that is only internal to the local network (we assume you trust your networks, otherwise you won't have non encrypted services).

Just to give you a point of comparison: if you open an external port of your Router to reach your local WebCam over an HTTP channel (statistically speaking, there is a large number of people out there doing this!), your entire communication between the client (e.g. Web Browser) and the WebCam is in clear: so, anybody in the middle can sniff the traffic and look at your WebCam.

Secondly, consider local services not even protected by a password, but exposed over internet through the same mechanism (NAT on the Router: have a look at this article). This is yet another way in which your network can be exposed to vulnerabilities.

With Domotz's mechanism, you simply cannot sniff that traffic. Moreover, as stated above, with Domotz's solution you do not need to open any incoming port on the Router, Firewall or Modem to access your devices remotely; as a matter of fact, opening ports on the Router for the WAN side (which usually do not offer trusted security features) increase the risks of being attacked, since most of the malicious attacks start from a scan of the potential attack surface.

Moreover, if you look at the URL when opening a Remote Connection through the WebApp, and you copy and paste that URL on a different PC/Client, you will not be able to reach the end-device.

This has been designed in order to allow people to use the Domotz App even in a non-secure location: e.g., if you are in an Internet Cafe', over a non-secure WiFi, anybody with a little bit of IT skills can identify the URL you are connecting to (even if it is over HTTPS). But with only that URL, the hacker cannot reach your remote monitored networks and devices.

Finally, the Domotz solution for the direct Remote Connectivity guarantees an additional level of security, given that all the supported protocols are encrypted when the data is exposed on the public network. Therefore, even the data for the Telnet and Http Remote Connection (which, by default, are not encrypted), with the Domotz solution are secured on the public network by this encrypted channel.

Moreover, we have also provided a very secure way to connect to remote devices through a non-directly supported protocol (e.g. FTP, VNC, and in general any proprietary TCP protocol). Even though the Open TCP Tunnel functionality does not guarantee the same level of encryption as the direct Remote Connectivity, we have protected the end–point of the secure channel allowing only connections coming from the specific calling public IP (which is the public IP of the client initializing the Remote Connection).

PDUs/Smart Plugs, PoE Switched, device passwords and SNMP community strings

Some PDUs, Smart Plugs, PoE Switches or generic driver-supported devices are password protected (or require certain SNMP community strings). In order to allow our users to remotely control their devices, we ask through the App the credentials (or community string) to act on that specific device. The credentials are transmitted to our Cloud over a secure channel (HTTPS), and from our Cloud to the Agent over a secure channel as well (AMQPS).

In order to have a better experience, we ask for the password just one time (unless you change the password on your device, of course). However, we do not store the password in clear text in our Cloud. We store the password encrypted and password protected, so that a possible hacker attack which might get access to the database (though we believe nobody will be able to do that), will never be able to decrypt that password.

Credit Card numbers

We do not store your credit card numbers in our infrastructure for any reason. We rely on a secure, and well known service for payment services (Digital River, Inc., Stripe, etc.). Other very well-known companies rely on the same services: just to name a couple of them, Microsoft, Amazon, Spotify, Allianz, Adobe, Cisco and Lenovo.

Updates to this document

August 10th 2016	Version 1.0
September 22nd 2017	Version 1.1
May 21st 2018	Version 1.2
October 8th, 2018	Version 1.3