DOMOTZ SECURITY

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

Domotz 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 bodies 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 in as other mainstream cloud service, such us iCloud or Dropbox. We actually built our cloud solution on top of the best and most common practices with regard to security: as compared to other competitors in the same market (Home Automation), we believe that we have also stressed more than others on the 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. We also plan to introduce enhanced security features in the future to notify you, amongst other things, of abnormal or suspicious activity in your network, which I think you will really appreciate.

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

Cloud Infrastructure

The Domotz 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 level 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.

Finally, we have engaged external and independent bodies to perform continuous security assessments and penetration testing in order to guarantee the highest level of security for our cloud solution.

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, Raspberry Pi or your private NAS) connects to our cloud with a different credential set (see below). So you will not even find your main password on the device.

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 to 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 home 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 in any moment you want, so that the invited guest can't 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 plugs, 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's only stored on premises on your Domotz device - e.g. Raspberry Pi or NAS).

As said before for the Client Communication channel, we do not store the Agent password in clear 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 Home Network, since all the communications are established from within the Home Network toward the cloud. It creates encrypted and temporary overlay networks from within the Home Network to the Cloud. Therefore, no additional ports should be opened to the outside.

Remote Connect functionality

When clicking the Remote Connection (it is either HTTP or HTTPS, SSH or Telnet, RDP or VNC), we establish a secure channel (Encrypted Overlay Network) between your home network and our cloud and an HTTPS channel between the App (either Mobile App or WebApp). So the entire communication from the App to the Agent is encrypted (and 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 network, otherwise you won't have non encrypted services).

Just to give you a term of comparison: if you open an external port of your Router to reach your local WebCam over an HTTP channel (believe me, there is a huge number of people out there doing this), your entire communication between the client (Web Browser for example) and the WebCam is in clear: so, anybody in the middle can sniff the traffic and look at your WebCam.

We won't even mention 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).

With our mechanism, you simply can't sniff that traffic. Moreover, as stated above, with Domotz solution you do not need to open any port on the Home Router to access your home devices remotely; as a matter of fact, opening ports on the Router (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 won't 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 can't reach your home device.

Finally, the Domotz solution for the 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 channels.

PDUs, Smart Plugs and SNMP community passwords

Some PDUs, or Smart Plugs or SNMP devices are password protected. In order to allow our users to remotely control their devices, we ask through the App the user/password to act on that specific device. The user/password is 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 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 no-body 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 (BrainTree - part of PayPal group). Other very well-known companies rely on the same service: just to name a couple of them, airbnb and uber.

Updated Aug. 10th 2016