MANUALE OPERATIVO PIATTAFORMA IOT LOGBOT

Versione 3.0

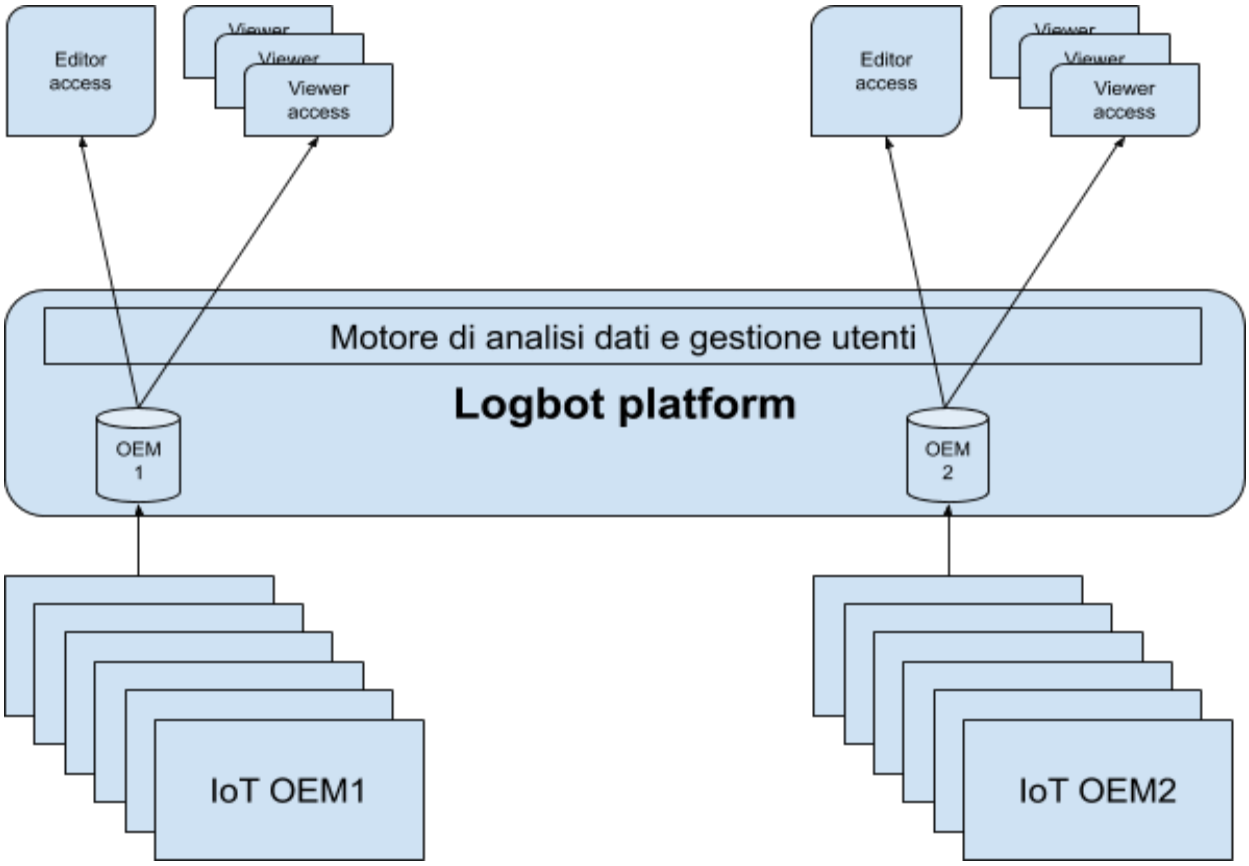
OVERVIEW ED INTRODUZIONE

Architettura del sistema

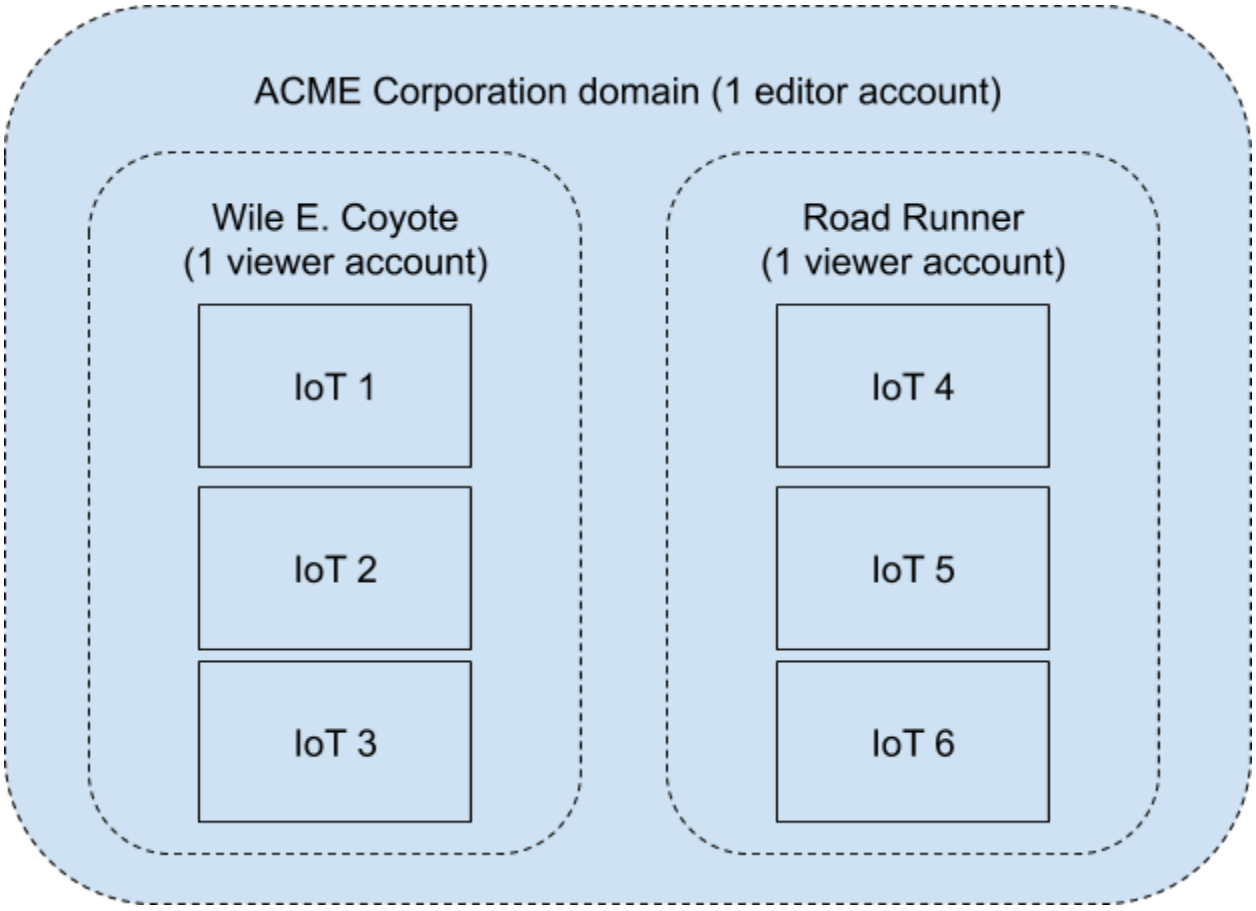
La piattaforma Logbot permette la gestione di flotte di dispositivi IoT per raccolta dati e teleassistenza di macchinari industriali e sistemi di automazione industriale e civile in generale, garantendo la sicurezza del dispositivo stesso e dei dispositivi connessi.

La piattaforma è costruita con una logica di multi-tenancy, dove per ogni OEM che deve gestire una flotta di IoT è creato:

- un database ridondato dove vengono memorizzati i dati raccolti dalla propria flotta
- un accesso al portale come “Editor”, dove può gestire i propri dispositivi IoT, creare dashboard per l’analisi dei dati ed amministrare gli accessi VPN per la teleassistenza sui sistemi di automazione
- Un mini-portale di registrazione degli utenti “Viewer”, ovvero i clienti dell’OEM ai quale quest’ultimo può fornire accesso ai dati ed alle analisi/dashboard relative alle loro installazioni.



Ad esempio: ACME Corporation costruisce macchinari industriali dotati di dispositivi IoT, l'IoT manager di ACME Co. avrà un account "Editor" dove poter gestire i propri dispositivi (e quindi la flotta di macchine installate), creare dashboards per sé e per fornire servizi quali manutenzione predittiva o monitoraggio della produzione ai propri clienti (Wile E. Coyote e Road Runner), che registrerà come utenti "Viewer" ed ai quali assegnerà dashboards per visualizzare lo stato delle proprie macchine.



Overview dell'ambiente

Utenti

Logbot mette a disposizione due livelli di utenti: utenti editor ed utenti viewer. Ogni utente editor ha giurisdizione sul proprio tenant, ovvero sui propri IoT che ha configurato, sui dati generati raccolti da questi, sugli utenti viewer della propria organizzazione e sulle dashboard che ha creato.

L'utente viewer che è stato creato da un editor ha accesso soltanto alle dashboard che gli sono state assegnate, e senza possibilità di modificarne il contenuto.

Dashboard

La dashboard è un gruppo di pannelli che compaiono su un'unica pagina web e che condividono un intervallo di tempo selezionato tramite l'apposito controllo localizzato sempre in alto a destra per ogni dashboard.

Le dashboard hanno la possibilità di utilizzare le funzionalità di templating per renderle più dinamiche ed interattiva.

E possibile creare annotazioni sui pannelli per marcare e taggare particolari eventi, che possono poi essere ritrovati e filtrati su altri pannelli o dashboard. Esse sono anche utili per correlare eventi e metriche su pannelli diversi contenuti nella stessa dashboard.

Dashboards e pannelli possono essere condivisi tramite link univoco generato dal pannello stesso che può essere inviato tramite email ad esempio.

Le dashboard possono essere taggate, copiate, esportate e lo storico delle modifiche è mantenuto per permettere un facile recupero delle stesse.

Le dashboard ed il loro contenuto sono automaticamente scalati per adattarsi alla risoluzione del browser, dallo smartphone alla TV.

Pannelli

Il pannello è il blocco base con cui costruire le dashboard, ogni pannello mette a disposizione un generatore di query per interrogare il database delle proprie metriche ed effettuare le analisi, ed un tool per selezionare il tipo di grafico: da semplici istogrammi, torte, tabelle a più avanzati strumenti di visualizzazione.

I pannelli possono essere spostati e ridimensionati a piacere, ed organizzati in sezioni chiamate "row".

SETUP DISPOSITIVO IOT2040

Funzionalità supportate

Il dispositivo IoT consente la raccolta di dati da PLC e dispositivi sul campo che supportano i seguenti protocolli di comunicazione su base ethernet: S7 protocol, OPC-UA e Modbus TCP. Ogni dispositivo può essere abilitato, in modo reversibile, a comunicare in uno dei protocolli sopra indicati con al più 6 dispositivi, raccogliendo un numero di parametri complessivo non superiore alla taglia acquistata. Il formato di dato raccolto può essere deciso per parametro e sono supportati valori numerici di tipo BOOL,INT,REAL... fino ad un massimo di 64 bit e con frequenza di campionamento non inferiore ai 10s e non superiore a 1g. Per ogni dispositivo iot vengono anche inviati parametri sullo stato di funzionamento del dispositivo stesso e delle connessioni verso i dispositivi sul campo; tali parametri sono consultabili e non vengono conteggiati sul complessivo dei parametri che prevede la licenza. Il dispositivo iot richiede la sola configurazione delle porte ethernet e della chiave di licenza per essere operativo. La configurazione della comunicazione, dei parametri acquisiti... viene automaticamente ed istantaneamente sincronizzata dal cloud senza alcun intervento sul campo. Il dispositivo monta due porte ethernet per isolare la rete OT (campo) dalla rete IT separate internamente da un firewall che garantisce la sicurezza di tutti i dispositivi del campo connessi ad essa, nonché del dispositivo iot stesso. E` possibile instaurare una connessione vpn verso ogni dispositivo iot della propria flotta da qualunque PC Windows sul quale sia installato il client VPN. La vpn consente di accedere in modo sicuro ai dispositivi sul campo per effettuare teleassistenza, instaurando un bridge layer2 tra IoT e PC permettendo di effettuare tutte le azioni come se si fosse collegati direttamente alla rete locale OT. L'aggiornamento dei dispositivi iot è completamente gestito dalla piattaforma, che si occupa di rilasciare in modo completamente trasparente patch di sicurezza e nuove funzionalità su tutti i dispositivi IoT connessi.

Contenuto della confezione

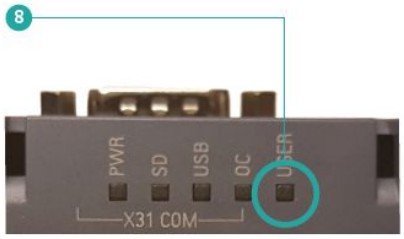
La confezione contiene la scheda microSD pronta per essere inserita nel dispositivo iot2040, una breve guida di getting-started, e la chiave di licenza (token) per registrare il dispositivo iot sulla piattaforma cloud.

Installare la scheda SD su IoT2040

Per installare la scheda microSD sul dispositivo iot estrarla dal suo adattatore, alzare lo sportellino sul fronte destro del dispositivo ed inserire la scheda nell'apposito alloggiamento facendo attenzione a non forzare la slitta ed assicurandosi che combaci completamente con i contatti alla base. Richiudere la slitta e successivamente lo sportellino frontale.

Installazione dell'IoT2040

Il dispositivo iot2040 deve essere alimentato a 24 volt tramite il connettore sul lato superiore. Può essere inserito su guida din rispettando le indicazioni fornite dal costruttore. La porta ethernet X1 è dedicata alla connessione verso il campo, la porta X2 è invece dedicata alla connessione verso la rete IT (internet). Le porte sono entrambe Fast Ethernet con supporto per auto MDI-X. Il dispositivo iot dispone di alcuni led che ne indicano lo stato di funzionamento: il primo led sulla sinistra indica la corretta alimentazione, il secondo indica attività in lettura/scrittura su microSD e lampeggerà in fase di avvio ed aggiornamento del sistema. L` ultimo led (user 8) sulla destra comunica la corretta configurazione e connessione del dispositivo, seguendo la codifica sottostante.



Una volta riavviato l` iot2040 il led di configurazione risultera ` spento nel caso la procedutra sia avvenuta con successo. Differenti stati del led possono fornire informazioni aggiuntive:

- **rosso fisso**: non configurato
- **rosso lampeggiante**: configurato non con nesso a internet
- **spento**: configurato e connesso

Sotto lo sportellino di destra è presente un pulsante per effettuare il reset del dispositivo; fare attenzione a non premere il pulsante quando si applica la maschera se si installa il dispositivo in un quadro.

Steps

Estrarre la scheda MicroSD dal proprio alloggiamento:

Aprire lo sportello destro del dispositivo IoT:

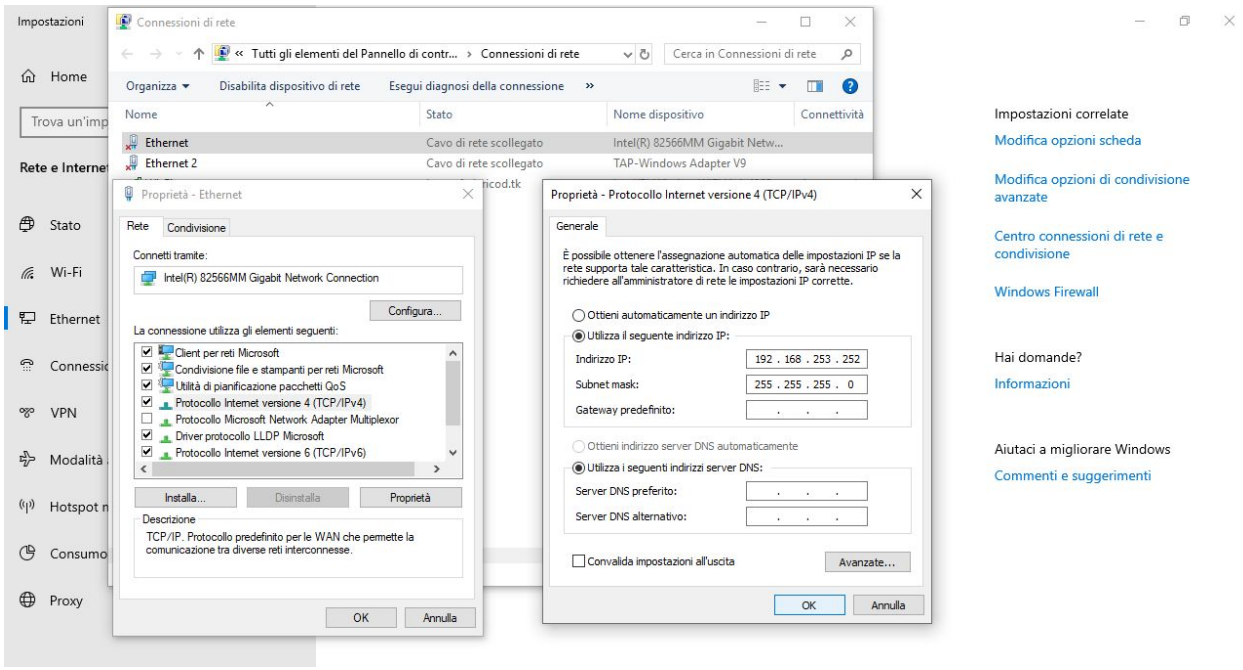
Inserire la scheda MicroSD nell’apposito alloggiamento:

Primo avvio dell'IoT2040 e connessione ad un servizio di telemetria

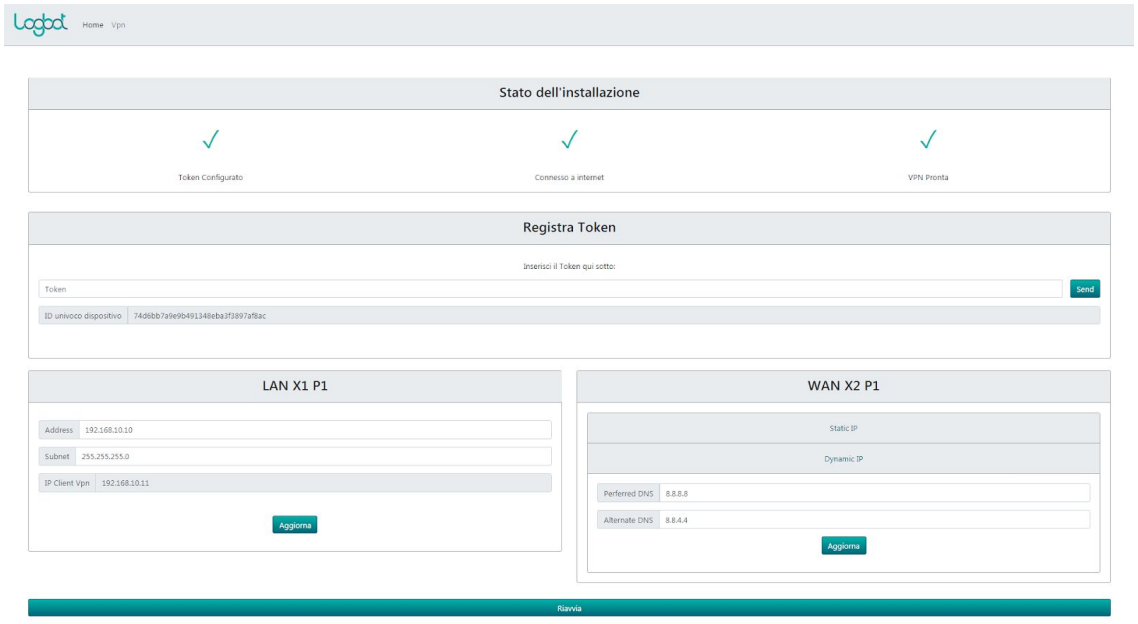
Al primo avvio il dispositivo sarà raggiungibile sulla porta X1 all'indirizzo 192.168.253.252 . Per accedere, impostare la scheda di rete del pc sulla rete 192.168.253.x con maschera 255.255.255.0 e connettersi tramite browser all'indirizzo http://192.168.253.252/ . Sulla pagina impostare l'indirizzo ip e la maschera di sottorete per la rete di campo (LAN) e per la rete IT (WAN), la connessione verso internet verrà automaticamente testata dal dispositivo ogni 5 secondi, ed il suo stato verrà fornito sotto il tab ‘Stato dell'installazione’ nella voce ‘connessione’. Successivamente inserire il token di licenza ricevuto nella confezione e premere il pulsante di conferma (All` interno della confezione sono disponibili due copie del manuale). Infine premere il bottone di reboot sull interfaccia web ed attendere il riavvio dello stesso. Il riavvio potrebbe richiedere fino a 5 minuti, attendere fino al completamento, in caso di procedura avvenuta correttamente il led di ‘user’ dovrebbe risultare spento (in caso contrario fare riferimento alla codifica del led user disponibile nel paragrafo precedente). A questo punto il dispositivo e sincronizzato con la piattaforma cloud ed e pronto a ricevere la configurazione e gli eventuali aggiornamenti. Disconnettere quindi il pc, da adesso non sara piu necessario accedere fisicamente al dispositivo e sarà possibile effettuare ogni operazione direttamente dal portale in cloud.

Steps

Configurare l’interfaccia di rete del proprio PC:



Accedere alla pagina di configurazione dell’IoT2040 ed impostare indirizzi LAN/WAN, successivamente verificare la connessione di rete e registrare il token, infine premere il pulsante di riavvio:

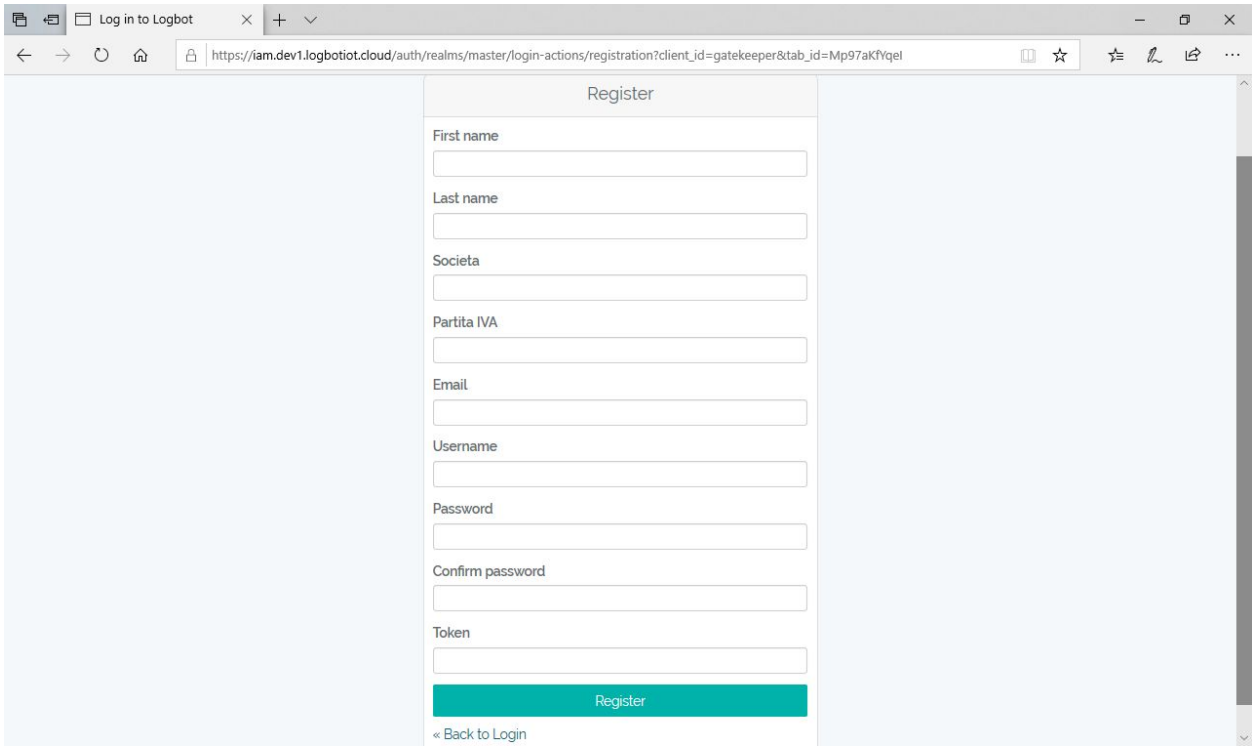


ONBOARDING DI IOT2040 SU LOGBOT

Onboard del primo IoT e registrazione sul portale

Per effettuare l'onboarding del primo IoT e necessario registrarsi al sito https://platform.logbotiot.cloud/ inserendo Nome e Cognome dell'amministratore, nome della Societa, P.IVA, email, username e password. Inoltre per la registrazione e necessario possedere un token di licenza IoT (nel formato xxxxxxxxxxxx.yy), l'IoT inserito sara registrato e sarà il primo IoT configurato disponibile.

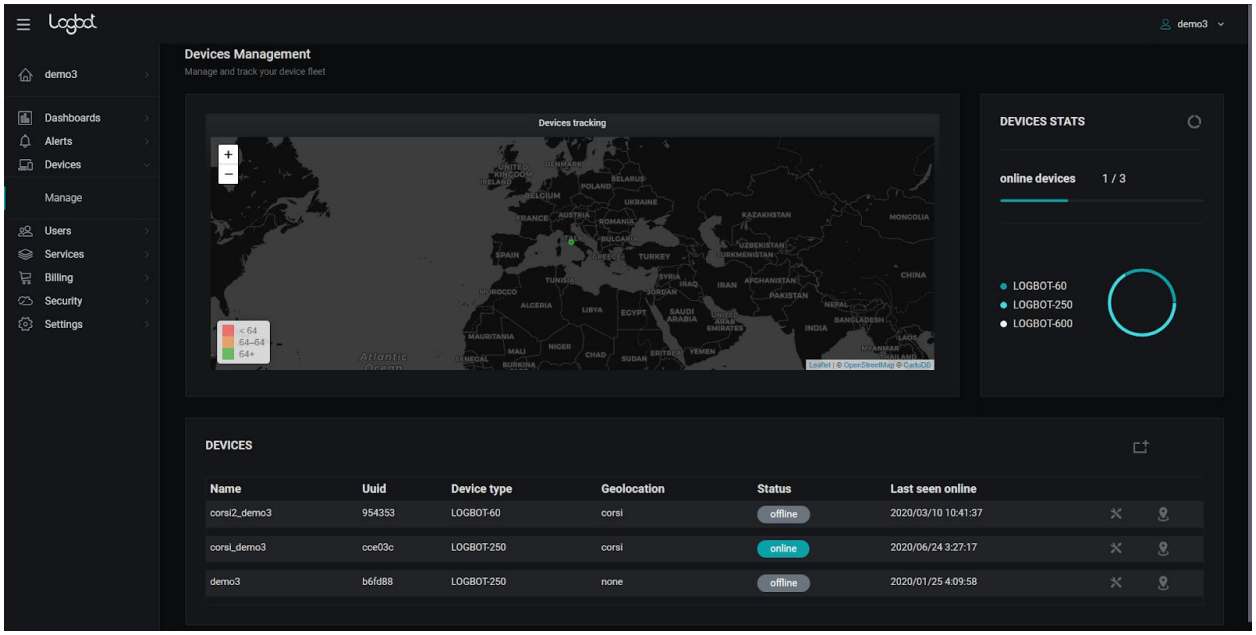
Cliccare quindi sul pulsante "Register", e controllare la casella di posta per l'email di conferma.



Onboard dei successivi IoT

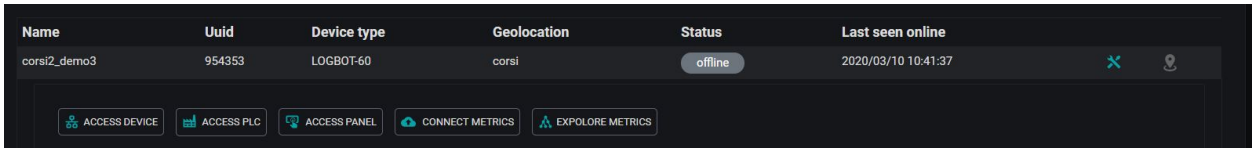
Logbot mette a disposizione una pagina (Devices > Manage) per la gestione dei propri dispositivi IoT. Ogni dispositivo IoT è contraddistinto da un nome univoco che lo identifica anche nell'ambiente di sviluppo delle dashboard, un codice denominato UUID, necessario in caso di supporto, una location, stato di funzionamento, e la data dell'ultima connessione del dispositivo alla piattaforma.

Per registrare un nuovo IoT è necessario entrare nella pagina Manage e cliccare il bottone "Add device"  , inserire quindi le informazioni necessarie: nome identificativo dell'IoT, token di licenza (nel formato xxxxxxxxxxxx.yyy). É possibile definire il luogo di installazione cliccando il bottone  .



Configurazione e test degli IoT

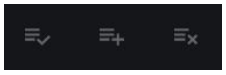
Per configurare e riconfigurare i dispositivi IoT registrati cliccare sul bottone  , si aprirà un menu dove è possibile utilizzare le funzionalità attive sull'IoT selezionato.



Per configurare l'acquisizione dati cliccare "Connect Metrics", si aprirà una pagina dove è possibile configurare le connessioni verso i PLC.

Aggiungere una connessione cliccando su 

e parametrizzarla configurarndo il nome del PLC, l'indirizzo IP (che dovrà essere nella stessa sottorete configurata sulla porta LAN del dispositivo IoT), rack e slot (rispettivamente rack 0 e slot 1 per Siemens S7 1200 e 1500, e rack 0 e slot 2 per LOGO!, S7 300 e 400).

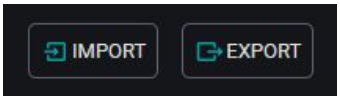
È possibile utilizzando i tre bottoni  modificare la connessione, aggiungere un parametro alla lista o eliminare la connessione.

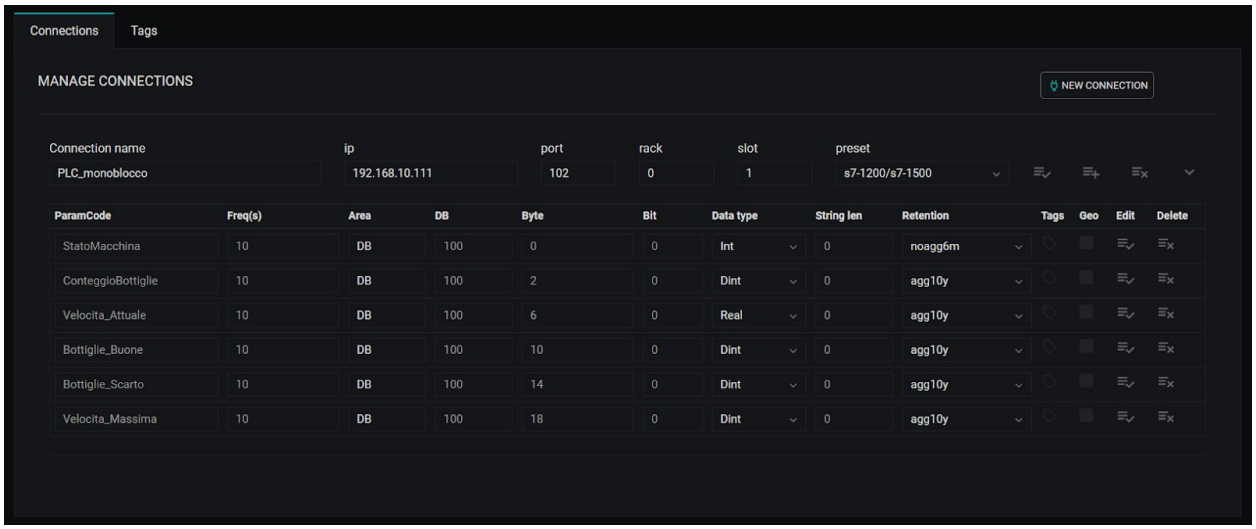
Aggiunti i parametri necessari inserire per ognuno il nome del parametro, la frequenza di acquisizione in secondi (maggiore di 5000), l'area di memoria, il numero della DB, il byte ed eventualmente il bit di start della lettura, il tipo di dato ed infine la retention policy da applicare:
- agg10y: dati mantenuti sul cloud per 10 anni ed aggregati
- noagg6m: dati mantenuti in cloud per 6 mesi non aggregati

Le funzionalità avanzate Tags e Geo permettono di settare tags statici o dinamici sul dato ed associare un tag di geolocalizzazione alla metrica.

Configurati i parametri accertarsi che nessuno di essi sia in modalità "edit" e trasferire la configurazione sul dispositivo IoT cliccando su 

.

È possibile esportare ed importare la configurazione tramite i bottoni 

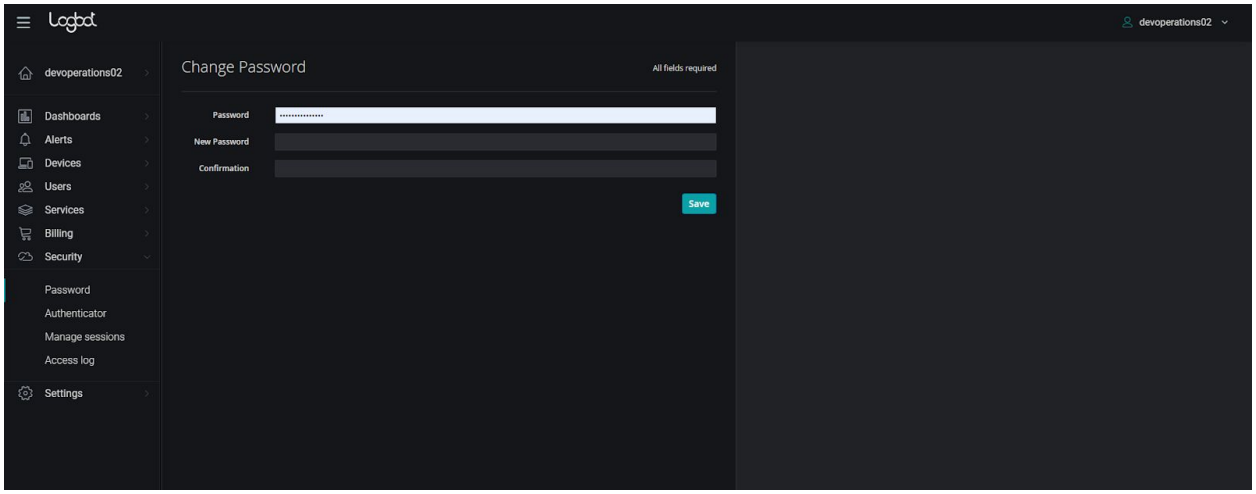

Connections
Tags
MANAGE CONNECTIONS
NEW CONNECTION
Connection name
ip
port
rack
slot
preset
PLC_monoblocco
192.168.10.111
102
0
1
s7-1200/s7-1500
ParamCode
Freq(s)
Area
DB
Byte
Bit
Data type
String len
Retention
Tags
Geo
Edit
Delete
StatoMacchina 10 DB 100 0 0 Int 0 noagg6m
ConteggioBottiglie 10 DB 100 2 0 Dint 0 agg10y
Velocita_Attuale 10 DB 100 6 0 Real 0 agg10y
Bottiglie_Buone 10 DB 100 10 0 Dint 0 agg10y
Bottiglie_Scarto 10 DB 100 14 0 Dint 0 agg10y
Velocita_Massima 10 DB 100 18 0 Dint 0 agg10y

Amministrazione del proprio account

Nel caso di perdita della password è possibile crearne una nuova tramite la procedura guidata di recupero password presente nella schermata di login.

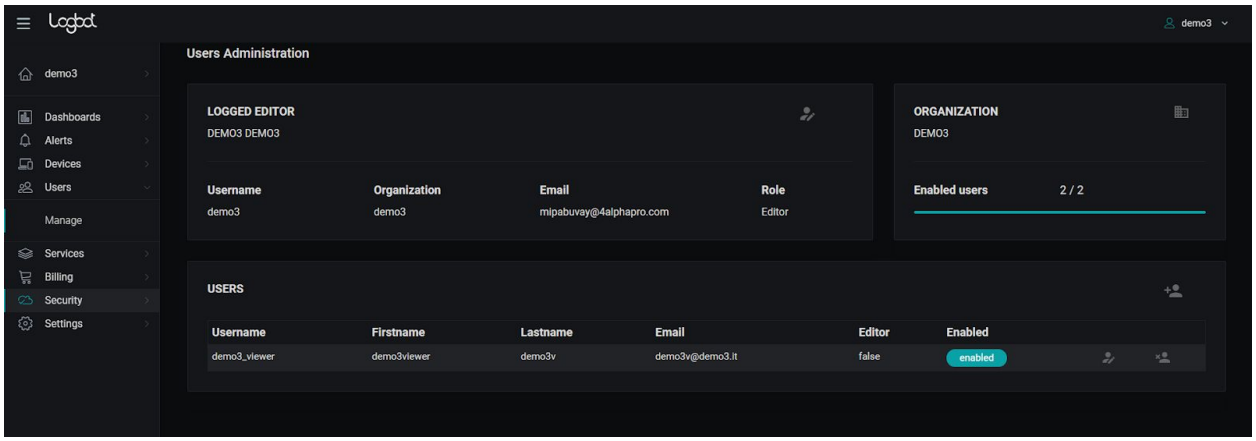
Ogni account editor o viewer ha accesso ad un pannello di gestione dell'account stesso dove è possibile riassegnare l'account ad un'altra persona fisica, cambiare l'email, modificare la password ed effettuare il logout da tutte le sessioni attive.

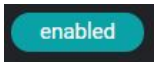
Queste pagine sono accessibili per entrambi gli account dal proprio portale (come da immagine) sotto il menu "Security".



Creare ed amministrare utenti

L’utente con ruolo di editor può creare ed amministrare utenti viewer dalla pagina “Users > Manage”. Per creare un nuovo utente cliccare su “Add user”  e seguire il wizard. Ogni utente è identificato con “username” ed email univoci, e compare nella tabella utenti.



È possibile abilitare o disabilitare ogni utente cliccando sul bottone 

.

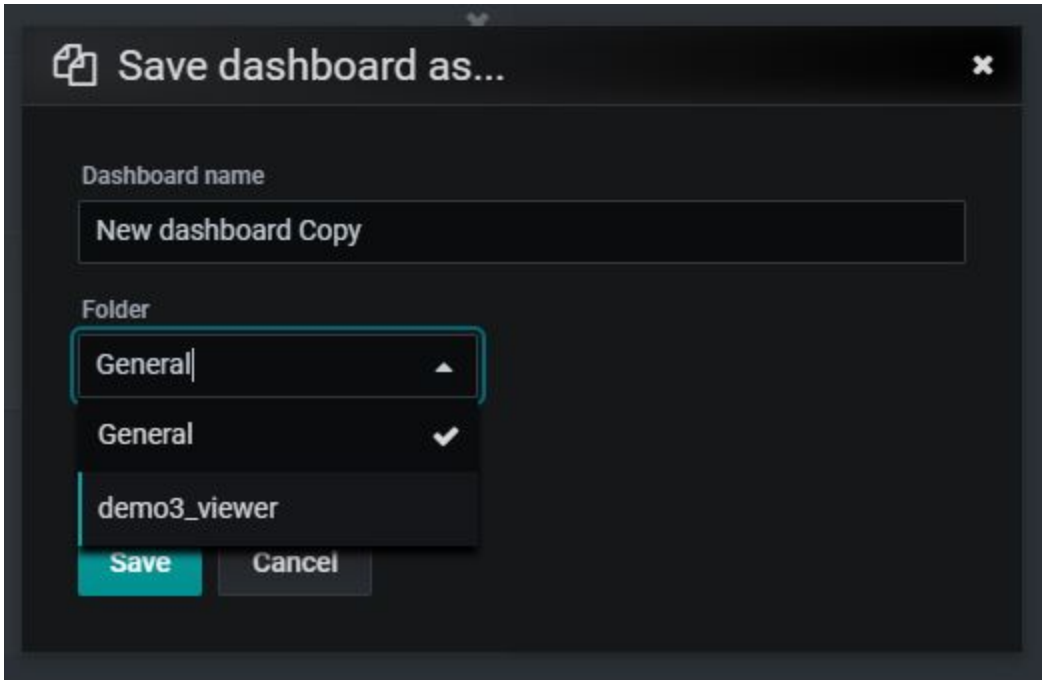
I bottoni  permettono di modificare ed eliminare l’utente rispettivamente.

REV: RACCOLTA, ELABORAZIONE E VISUALIZZAZIONE DEI DATI DEL CAMPO

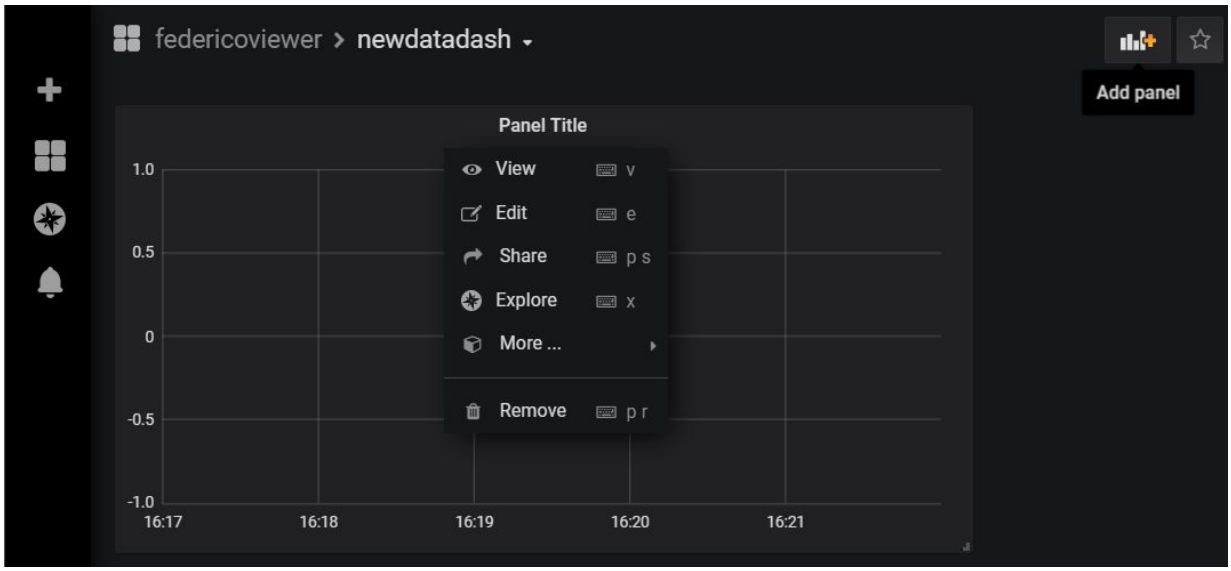
Creare la prima dashboard

Per creare la prima dashboard bisogna aver registrato almeno un utente viewer.

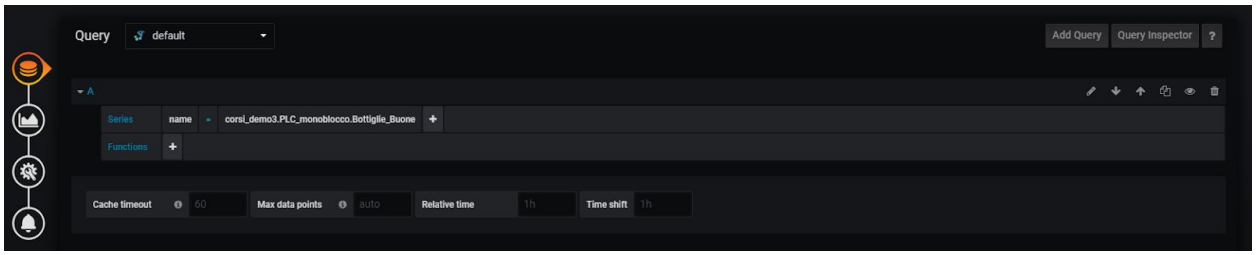
Creare una dashboard per quest'ultimo nella pagina "Dashboards > Create" e salvare la dashboard assegnandola all'utente viewer appena creato.



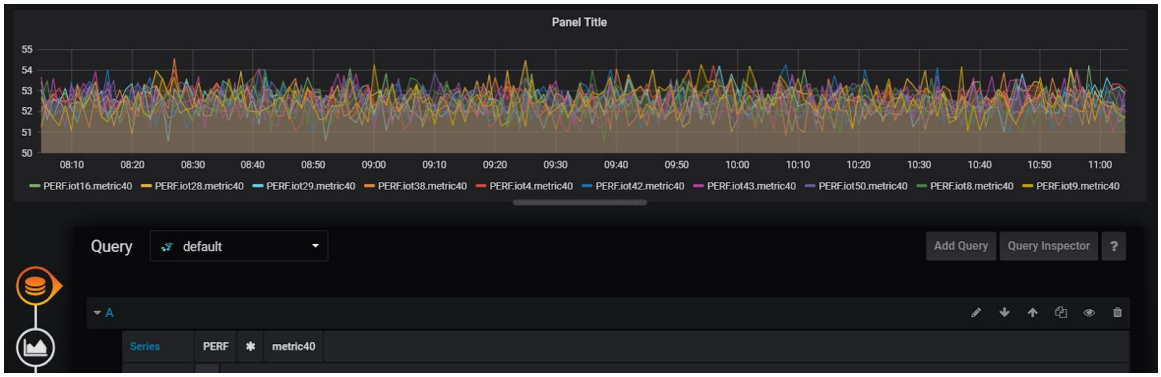
A questo punto cliccare sul pulsante  per aggiungere un pannello, selezionare poi "Add query" per editare la query. Cliccando su "select metric" è possibile navigare nella gerarchia dei dati selezionando il nome del tag che si vuole utilizzare come filtro.



Il tag “name” è disponibile per ogni dato e permette di accedervi utilizzando la gerarchia *nome_iot.nome_plc.nome_parametro*, secondo quanto configurato in precedenza nella sezione “Devices” del menu principale.



E` inoltre possibile applicare filtri ai dati in modo da poterli raggruppare tutti in un unico panel utilizzando una sola query. Nell'esempio sottostante osserviamo che il carattere wildcard (*) permette di ottenere la metrica del parametro metric4 per per un iot(sopra) e per tutti gli iot disponibili all'editor (sotto).



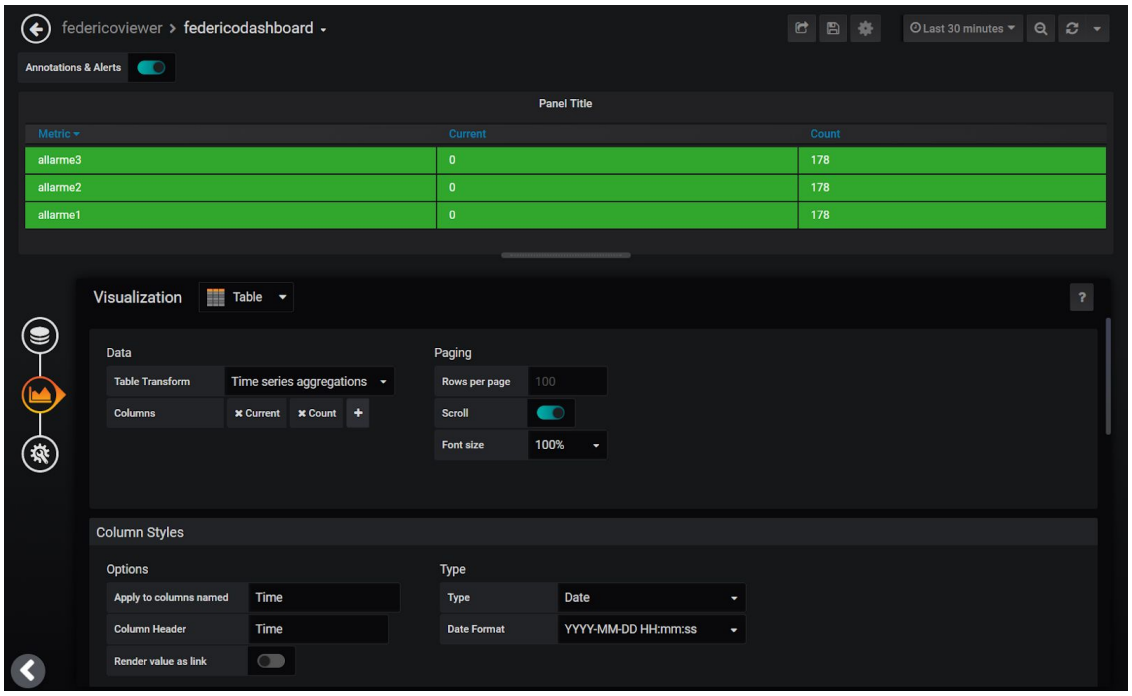
Cliccando su “Functions” e poi possibile applicare una o più funzioni di analisi al dato selezionato. E` disponibile un'ampia libreria di funzioni applicabili alle serie precedentemente create, che permettono di implementare funzionalità di aggregazione, nonché calcolo statistico e diagnostica avanzata sul proprio sistema.

Logbot utilizza il protocollo ‘graphite’ per implementare query e funzioni sulle metriche, per una panoramica completa sull` ampio spettro di funzioni supportate da graphite fare riferimento a https://graphite.readthedocs.io/en/latest/functions.html.

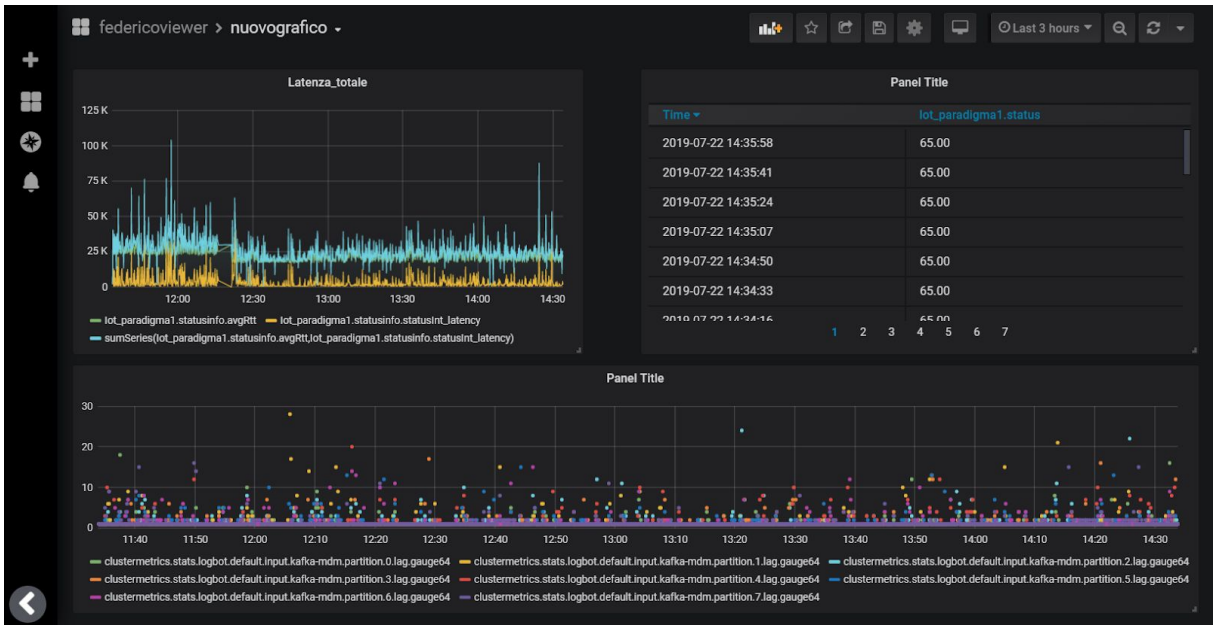
Nell'esempio sottostante andiamo a sommare due serie utilizzando la funzione ‘sumSeries’ andando a calcolare il tempo complessivo della latenza sull'invio del dato al sistema Logbot. Terminata questa operazione cliccare su “Visualization” e selezionare il tipo di visualizzatore e le relative proprietà. Infine tramite il pannello “General” e possibile inserire ulteriori informazioni sul pannello, come nome e descrizione del pannello.

E` possibile costruire anche altre tipologie di pannelli, tra cui heatmaps e tabelle, completamente configurabili a seconda dell’applicazione.

Vediamo un esempio di costruzione di una dashboard raffigurante il nome, stato attuale di tre allarmi e conteggio del numero di volte che tali allarmi si sono verificati, il tutto realizzato mediante un pannello tabulare. Selezionando il tipo di dato ALARM nella configurazione dei parametri iot da acquisire (sotto la pagina IoTs) , possiamo accedervi durante la creazione delle dashboard nella forma “nomeiot”.”nomeplc”.alarms.”nomeallarme” per creare una pagina come quella da esempio.



Una volta costruito il pannello, possiamo inserirlo all'interno della pagina di dashboard per costruire un'interfaccia di monitoring completamente personalizzabile con tutte le informazioni necessarie all` editor o richieste dal viewer del sistema.



A questo punto, essendo la dashboard configurata per uno specifico viewer, solamente quando quest'ultimo (o l'editor) si loggerà all'interno del sistema, potrà accedere alle dashboard ed alle informazioni presenti nella pagina configurata dall` editor.

In questo modo l'editor puo costruire dashboard personalizzate per i suoi viewers in modo completamente sicuro.

Politica di ritenzione dei dati

Le metriche ingerite dalla piattaforma Logbot sono accessibili ai suoi utenti per un periodo di tempo che arriva fino a 10 anni utilizzando la policy “agg10y” sulla singola metrica, con le precisazioni a seguire. I dati di più recente acquisizione sono anche generalmente quelli di maggiore significatività per estrapolare eventi ed effettuare classificazioni su possibili stati della sorgente del dato stesso. A questi si accede quindi con maggiore frequenza e la risoluzione del dato deve essere più elevata.

I dati più distanti nel tempo (più vecchi) sono invece più interessanti per le loro proprietà statistiche, che possono essere utilizzate al fine di desumere l'evoluzione futura del segnale, per questa ragione non e` necessario conservare i dati meno recenti con una risoluzione elevata.

Aderendo a questo principio guida, la piattaforma priorizza la ritenzione degli ultimi dati acquisiti, rispettando le politiche che seguono.

I dati risultano accessibili:

- Fino alla prima settimana con campionamento minimo a 10 secondi
- Fino al primo mese con campionamento minimo a 1 minuto
- Fino a 100 giorni a 10 minuti
- Fino a 5 anni a 1 ora
- Fino a 10 anni a 1 giorno

Nel momento del passaggio di un set di dati da un intervallo di ritenzione al successivo (per esempio un insieme di dati diventa più vecchio di una settimana) il sistema si occuperà di compattarli da un campionamento a 10 secondi ad uno di un minuto, assicurandosi durante il processo minimizzare la perdita di informazione preservando sempre all` interno del nuovo intervallo le seguenti tre proprietà`:

- Valore massimo nell intervallo
- Valore minimo
- Valore medio

È altresì disponibile una policy “noagg6m” che mantiene i dati in cloud per 6 mesi, non aggregandoli. Questa policy è utile nel caso debba storicizzare allarmi o stati macchina.

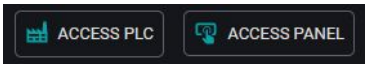
ACCESSO REMOTO AL DISPOSITIVO IOT ED AI DISPOSITIVI SUL CAMPO

Modalità di accesso remoto al campo

Sono disponibili due modalità di accesso al campo:

- Accesso VPN alla rete del dispositivo IoT per teleassistanza in layer 2 (è necessario un client VPN)
- Accesso tramite web browser alle pagine web dei dispositivi sul campo ed agli HMI che supportano il protocollo VNC (modalità proxy)

Accesso in modalità proxy

Per connettersi ai dispositivi sul campo accedere al proprio account, sulla tabella degli IoT premere il pulsante 

e selezionare il dispositivo a cui si vuole connettersi (PLC o HMI).

La connessione di tipo “PLC” permette di accedere alla pagina web di un qualsiasi dispositivo sul campo.

La connessione di tipo “HMI” permette di accedere ad un server VNC di un qualsiasi pannello operatore che supporti questa funzionalità.

Nel campo “IP” inserire l’indirizzo locale del dispositivo e la porta se diversa dalla 80 (default) in questo formato: IP:PORT.

Nel caso di connessione verso una pagina web la sessione scadrà automaticamente dopo 100 secondi di inattività.

Per connettesi direttamente al dispositivo cliccare il pulsante “Connetti”, per copiare un link univoco che, previa autenticazione, porterà l’utente direttamente alla pagina web del PLC o all’HMI utilizzare la funzione “Copia link diretto”.

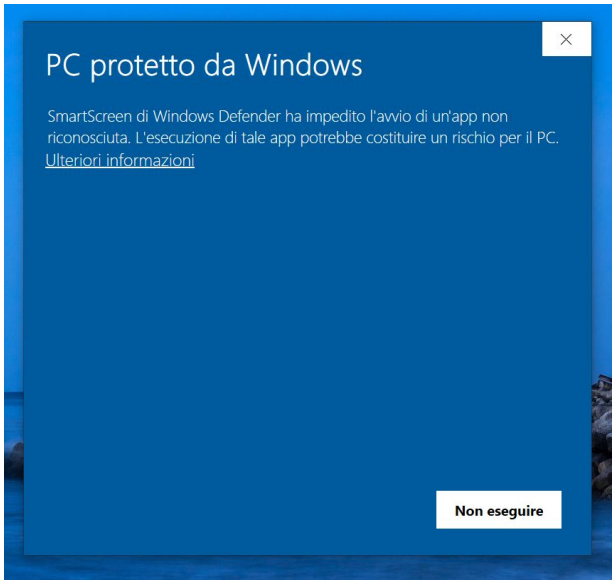
Client VPN

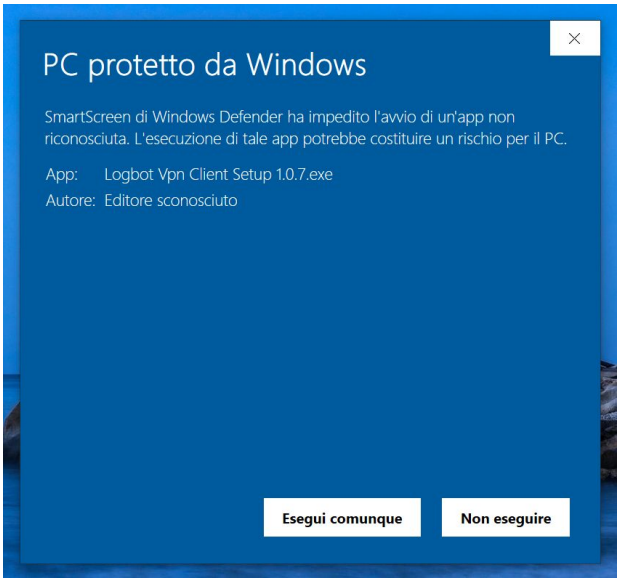
La connessione VPN necessita del software “Logbot VPN client” installato sul PC. Potete trovare il client aggiornato a questo indirizzo:

https://www.logbot.cloud/wp-content/uploads/2019/10/Logbot_vpn_client_full_installer_x64.exe

Installare il software selezionando tutte le componenti (Logbot VPN client, OpenVPN e TAP adapter).

Nel caso Windows non riconoscesse la provenienza del file selezionare “Ulteriori informazioni”, poi “Esegui comunque”:





Il software installa una interfaccia virtuale sul PC che sarà connessa in layer2 al dispositivo IoT, e che acquisirà l’indirizzo IP visualizzato nella pagina di configurazione dell’IoT.

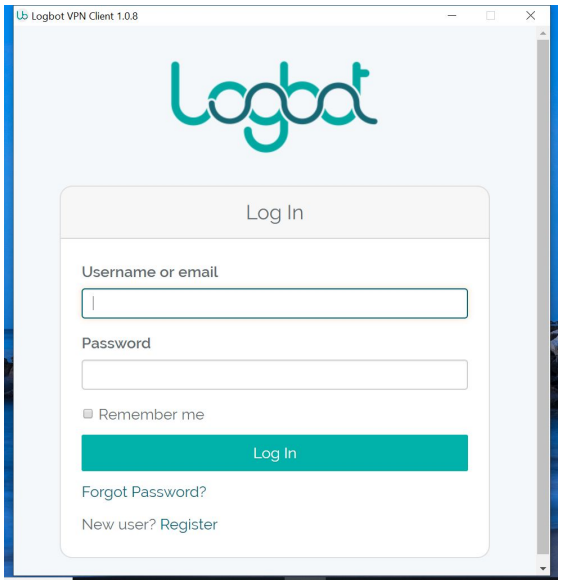
Per installare ed eseguire il software sono necessari i diritti di Amministratore su Windows.

Connettersi al dispositivo IoT in VPN

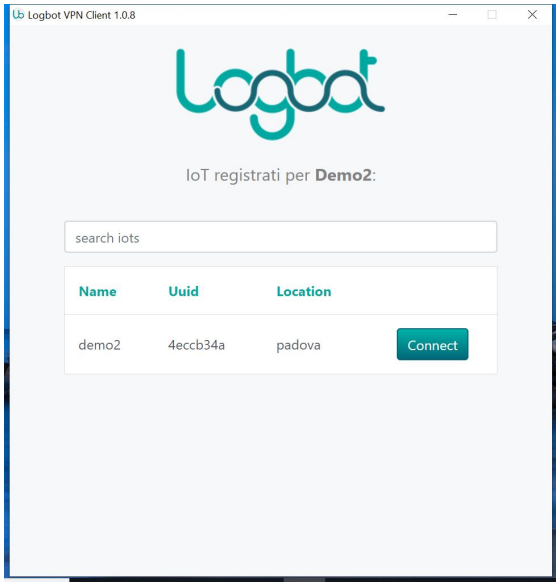
Per avviare la connessione, lanciare il client LBclient, effettuare la login tramite le credenziali dell'utente "Editor" e cliccare sul pulsante "Connetti" del dispositivo IoT al quale si vuole connettersi. I dispositivi offline avranno il pulsante disabilitato.
A questo punto è possibile interagire con i dispositivi sul campo tramite l'interfaccia TAP alla quale sarà assegnato automaticamente l'indirizzo IP visualizzato sulla pagina web dell'IoT (indirizzo IoT interfaccia LAN + 1, eg. se l'IoT ha indirizzo 192.168.1.1 il PC otterrà l'indirizzo 192.168.1.2).
Per disconnettersi cliccare sul pulsante "Disconnetti".

Steps

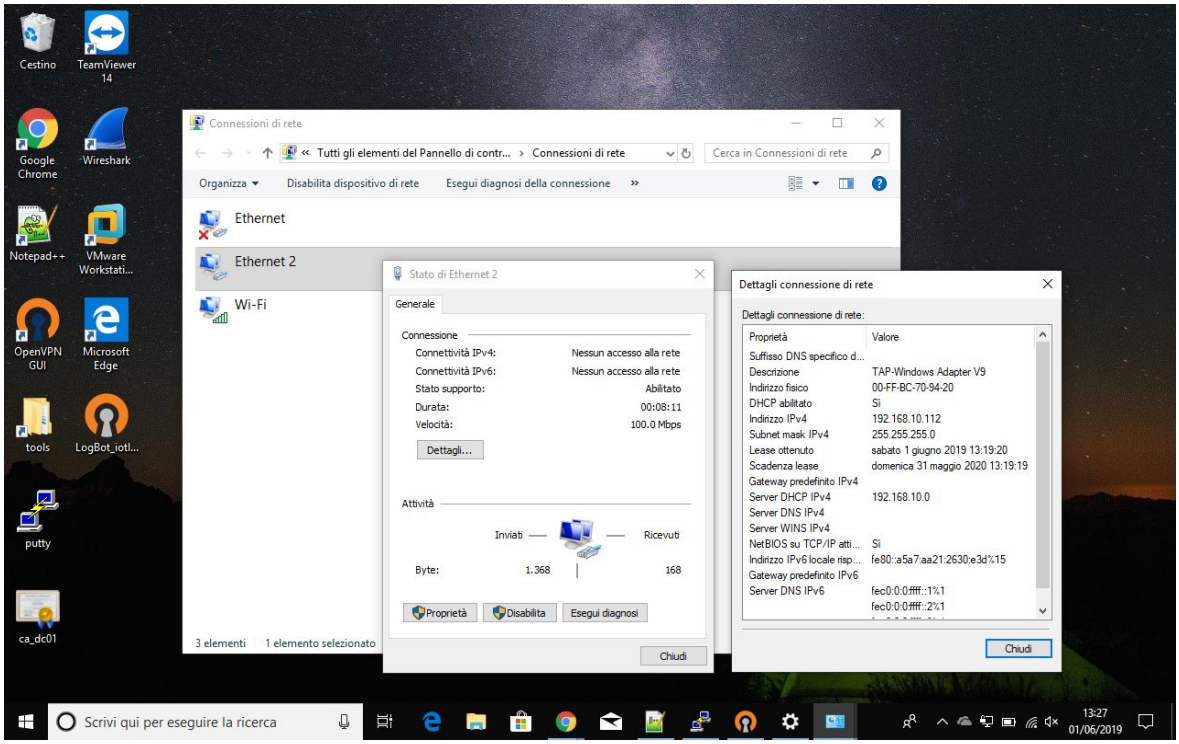
Lanciare LBclient ed effettuare la login



Connettersi ad un dispositivo IoT



Utilizzare l’interfaccia ethernet appena configurata come punto di accesso al campo:



Funzioni avanzate di connessione al campo

Logbot mette a disposizione una modalità avanzata di connessione tramite VPN che permette all’amministratore dell’account “Editor” di delegare una terza parte a connettersi al dispositivo IoT tramite VPN.

Per abilitare la connessione VPN entrare nella pagina di configurazione degli IoT e collegarsi al dispositivo IoT premendo il pulsante  . Si aprirà un tab sul vostro browser dove potrete scaricare il file di configurazione del dispositivo IoT selezionato premendo il pulsante Download.

Il file ha un nome parlante del formato: Logbot_<nome iot>_<versione>.ovpn, esso rimarrà valido fino a quando non verrà rigenerato o aggiornato l’indirizzo ip dell’interfaccia LAN.

In caso di necessità è possibile riavviare il servizio VPN sul dispositivo IoT premendo il bottone “Riavvia”, oppure rigenerare la configurazione premendo il bottone “Rigenera” e scaricando un nuovo file di configurazione. Rigenerando la configurazione viene anche rigenerata la chiave crittografica e viene quindi invalidato ogni file di configurazione precedentemente scaricato per quel dispositivo.

Per accedere ad un dispositivo IoT in VPN cliccare col tasto destro del mouse sul file di configurazione e selezionare la voce “Start OpenVPN on this config file”. Sul PC deve essere installato il software LBclient (oppure la versione Community di OpenVPN).

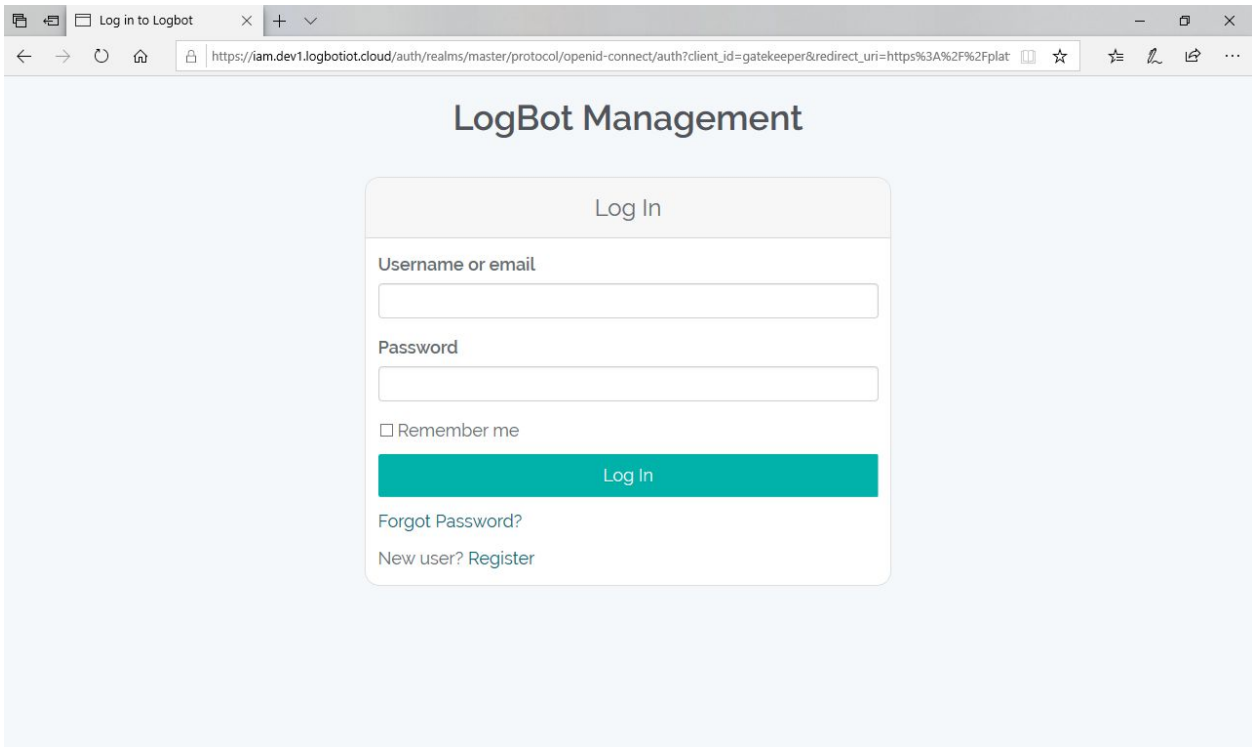
Si avvierà il client VPN, se la connessione avverrà con successo comparirà “Initialization Sequence Completed” sulla finestra del software VPN.

A questo punto è possibile utilizzare l’interfaccia ethernet virtuale come punto di accesso alla rete LAN del dispositivo IoT.

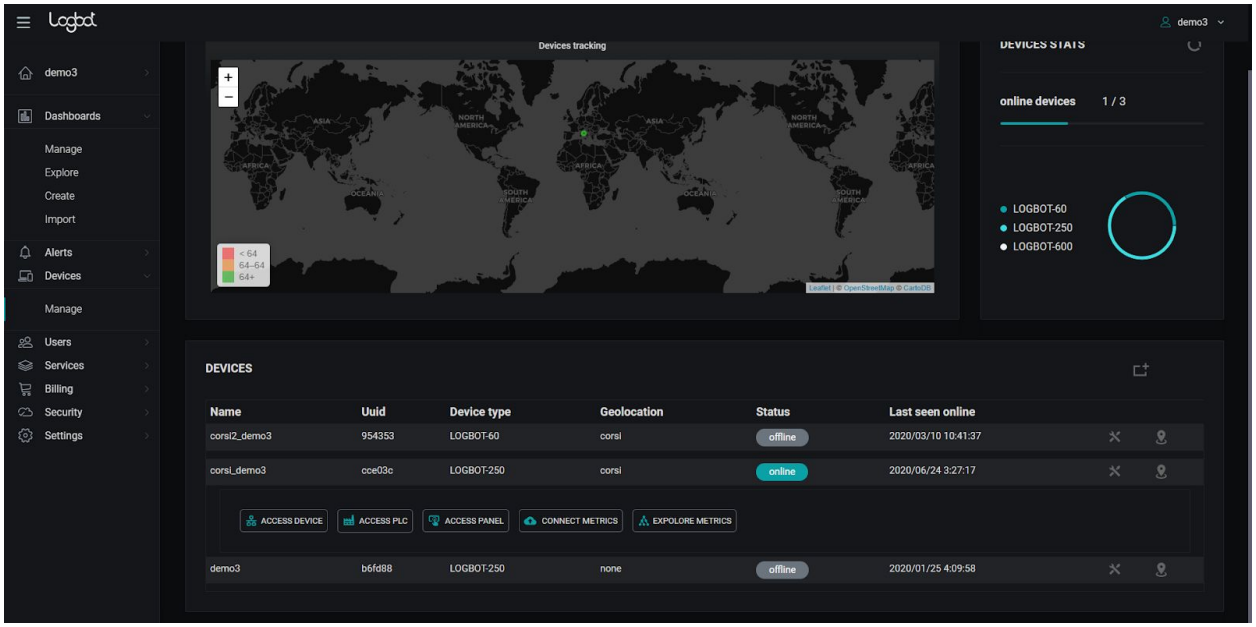
Per terminare la sessione chiudere semplicemente la finestra.

Steps

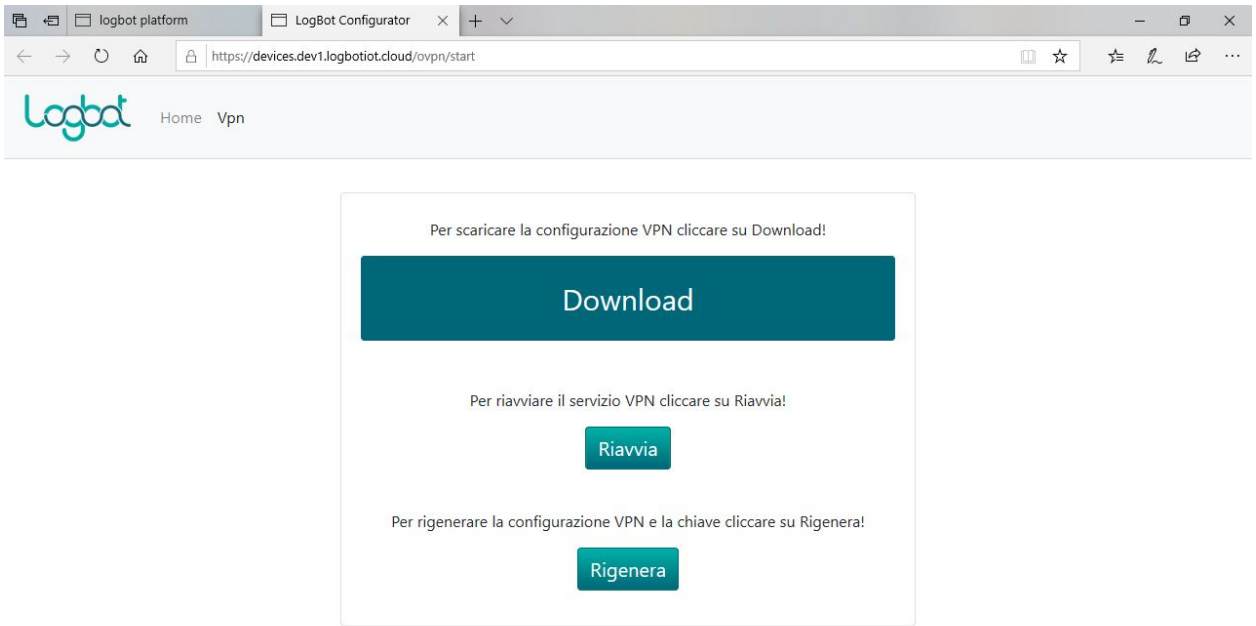
Accedere al portale Logbot:



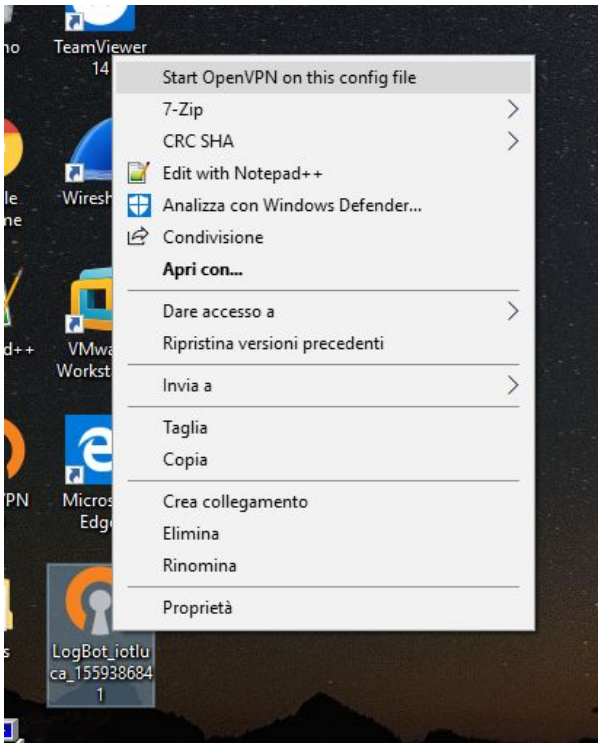
Selezionare il dispositivo IoT:



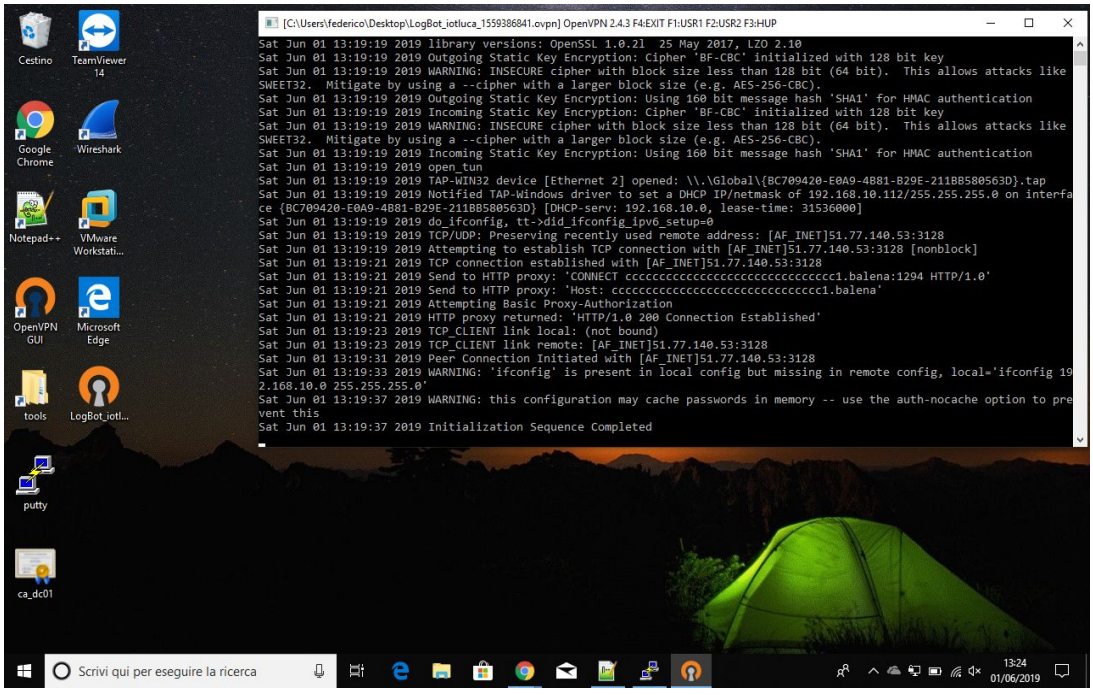
Scaricare il file di configurazione dalla pagina “Vpn”:



Avviare il client OpenVPN:



Attendere il completamento della connessione:



FUNZIONI AVANZATE DISPOSITIVO IOT

Reset dispositivo IoT

É possibile riportare il dispositivo IoT alle impostazioni di fabbrica entrando nella pagina “Avanzate” del dispositivo stesso.

Questa azione resetterà il token configurato, la configurazione della connessione VPN ed eventuali altre configurazioni effettuate sul dispositivo IoT, ad eccezione della configurazione di rete che rimarrà invariata.

Connessione ad un sistema di raccolta dati libero

É possibile connettere il dispositivo IoT ad un provider di raccolta dati libero, a condizione che questo rispetti alcune caratteristiche tecniche indispensabili. Si perderanno tutte le funzionalità di connettività VPN e di aggiornamento da remoto del dispositivo IoT.

Per configurare questa modalità registrare il dispositivo tramite il token di licenza ricevuto ed entrare nella pagina “Avanzate” del dispositivo IoT. Qui spuntare la checkbox “Attiva server Kafka libero (esperti)” ed inserire l’indirizzo del broker Kafka nel formato host:port (eg. kafka:9092 oppure 192.168.1.100:9092).

Caratteristiche richieste:

- Protocollo di comunicazione: Kafka
- Protocollo di incapsulamento dati: Messagepack
- Protocollo di incapsulamento configurazione: JSON
- Trasmissione dati: PLAINTEXT

Getting started:

1. Configurare un broker Kafka (ad esempio utilizzando il docker wurstmeister/kafka:latest)
2. Impostare i seguenti topic:
    - mdm
    - c2d-config-UUID
    - c2d-control-UUID
    - d2c-status-UUID
3. Sul topic c2d-config inviare la configurazione del dispositivo in formato JSON

Es:

```
{
  "OrgId": "1",
  "IOT_id": "iot1",
  "protocol": "s7",
  "TimeStamp": 1569589828246,
  "plc_array": [
    {
      "host": "192.168.10.111",
      "port": 102,
      "rack": 0,
      "slot": 1,
      "PLC_id": "Plc1",
      "data_array": [
        {
          "db": 1,
          "rw": "r",
          "area": "DB",
          "freq_ms": 10000,
```

```
          "ParamCode": "parametro_bool",
          "data_type": "X",
          "start_bit": 0,
          "start_byte": 8,
          "ParamDescription": "parametro_bool"
        },
        {
          "db": 1,
          "rw": "r",
          "area": "DB",
          "freq_ms": 10000,
          "ParamCode": "parametro_real",
          "data_type": "REAL",
          "start_bit": 0,
          "start_byte": 16,
          "ParamDescription": "parametro_real"
        }
      ]
    }
  ],
  "MessageVersion": "1.0.0"
}
```

4. Ricevuta la configurazione, il dispositivo IoT inizierà l'invio dei dati alle frequenza definita per ogni metrica, sul topic "mdm" in formato Messagepack

Schema:

```
type MetricData struct {
    Id       string   `json:"id"`
    OrgId    int      `json:"org_id"`
   Name     string   `json:"name"`
    Interval int      `json:"interval"`
    Value    float64  `json:"value"`
    Unit     string   `json:"unit"`
    Time     int64    `json:"time"`
    Mtype    string   `json:"mtype"`
    Tags     []string `json:"tags"`
}
```

INFORMAZIONI TECNICHE AGGIUNTIVE

Dispositivi compatibili con Logbot	Siemens IoT2040
Frequenza massima di acquisizione dal campo	10s
Numero massimo parametri	Secondo licenza: ● 60 per dispositivo IoT ● 250 per dispositivo IoT
Numero massimo PLC per dispositivo IoT	6
Protocolli di comunicazione verso il campo	S7 protocol
Policy ritenzione dati su piattaforma Logbot	agg10y: dati mantenuti sul cloud per 10 anni aggregati secondo la regola 10s:7d,1m:31d,10m:100d,1h:5y,1d:10y noagg6m: dati mantenuti sul cloud per 6 mesi, non aggregati
Funzioni di aggregazione per ritenzione	min,max,avg
Intervallo di tempo medio tra acquisizione e aggiornamento della metrica nel ring	60s
Formato esportazione dati	CSV

Formato esportazione configurazioni	JSON
Crittografia dati in transito	AES256
Tecnologia VPN	Layer2
Crittografia VPN	AES256
Connessioni VPN concorrenti	1 per dispositivo IoT
Protocolli supportati dalla modalità proxy	• HTTP • VNC
Tecnologia firewall	IPTABLES
Numero massimo utenti “Editor”	1
Funzionalità di sicurezza aggiuntive	• 2FA • MANAGED SECURITY UPDATES
Numero massimo utenti “Viewer”	Illimitati
Numero massimo Dashboards	Illimitate

Logbot effettua le seguenti connessioni TCP in uscita:

- invio metriche (TLS): **host** upstream.logbotiot.cloud **porta** 9092
- connessione vpn (TLS): **host** vpn.logbotiot.cloud **porta** 443 e 80
- telemetria (HTTPS): **host** api.logbotiot.cloud **porta** 443 e 80
- aggiornamenti (HTTPS): **host** registry.logbotiot.cloud **porta** 443 e 80