

Per attivare il servizio di parental control tramite il servizio “OpenDNS HomeFree”, è necessario seguire questi passaggi:

Creare un account su OpenDNS: prima di poter attivare il servizio, è necessario registrarsi su OpenDNS creando un account gratuito collegandosi al sito: <https://signup.opendns.com/homefree/>.

Ti ricordiamo che utilizzando il browser internet “Google Chrome” premendo con il pulsante destro del mouse sulla pagina internet è possibile tradurre la pagina in italiano

Prima di procedere con la procedura di registrazione si consiglia di andare sul sito: whatismyip.com e assicurarsi che appaia Etruriacom SRL


1. Inserire la propria e-mail,
2. selezionare la propria nazione
3. Creare una password (la password deve essere almeno 8 caratteri, contenere almeno una maiuscola, una minuscola, un numero e almeno un carattere speciale esempio: !, @, \$)
4. Premere il pulsante: “GET A FREE ACCOUNT”

🔒 <https://signup.opendns.com/homefree/>

You're just three steps away from a safer, faster, smarter and more reliable Internet — for free!

BENEFITS OF OPENDNS HOME

- ✓ Websites will load faster, and with OpenDNS' 100% up-time, you won't have to worry about unreachable websites and DNS outages from your ISP.
- ✓ With over 50 customizable filtering categories, OpenDNS Web content filtering keeps parents in control of what websites children visit at home.
- ✓ OpenDNS blocks phishing websites that try to steal your identity and login information by pretending to be a legitimate website. Surf the Web with confidence.
- ✓ Over 30,000,000 homes, schools, and businesses of all sizes rely on OpenDNS for a better Internet.

 Looking for threat protection?
[Learn more about Cisco Umbrella](#)

Already have an account? [Sign in.](#) All fields are required.

Email address

Confirm email address

Select your country

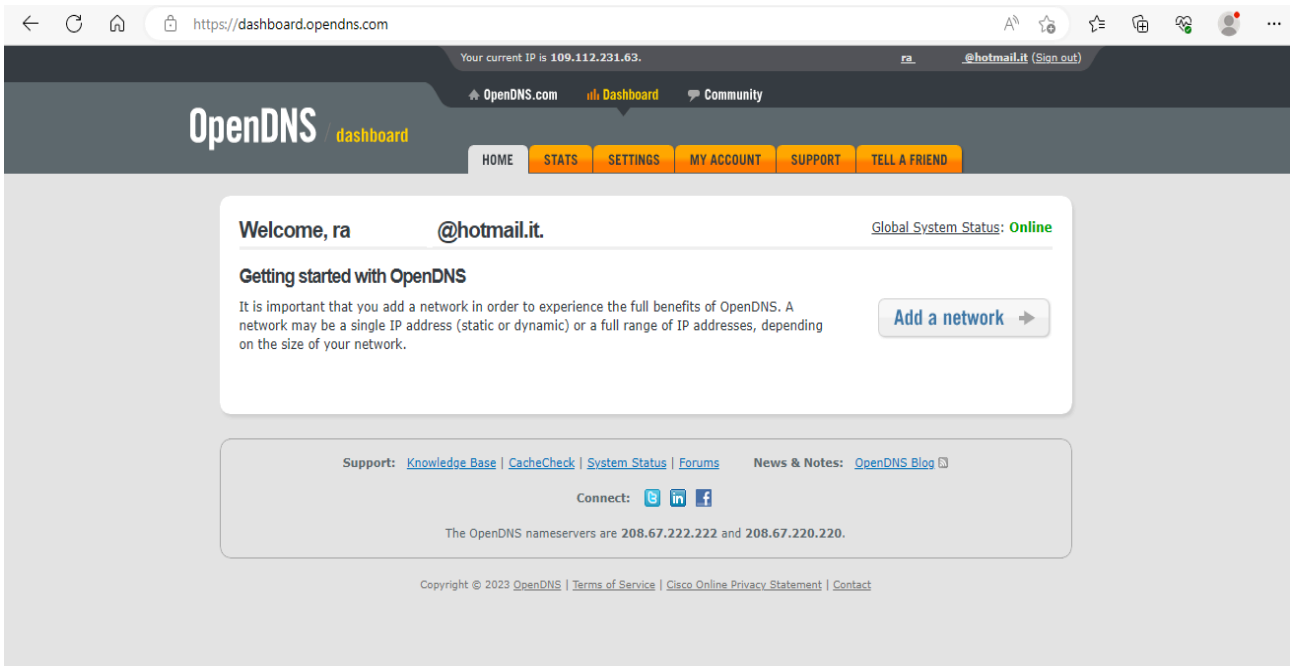
Create password

Confirm password

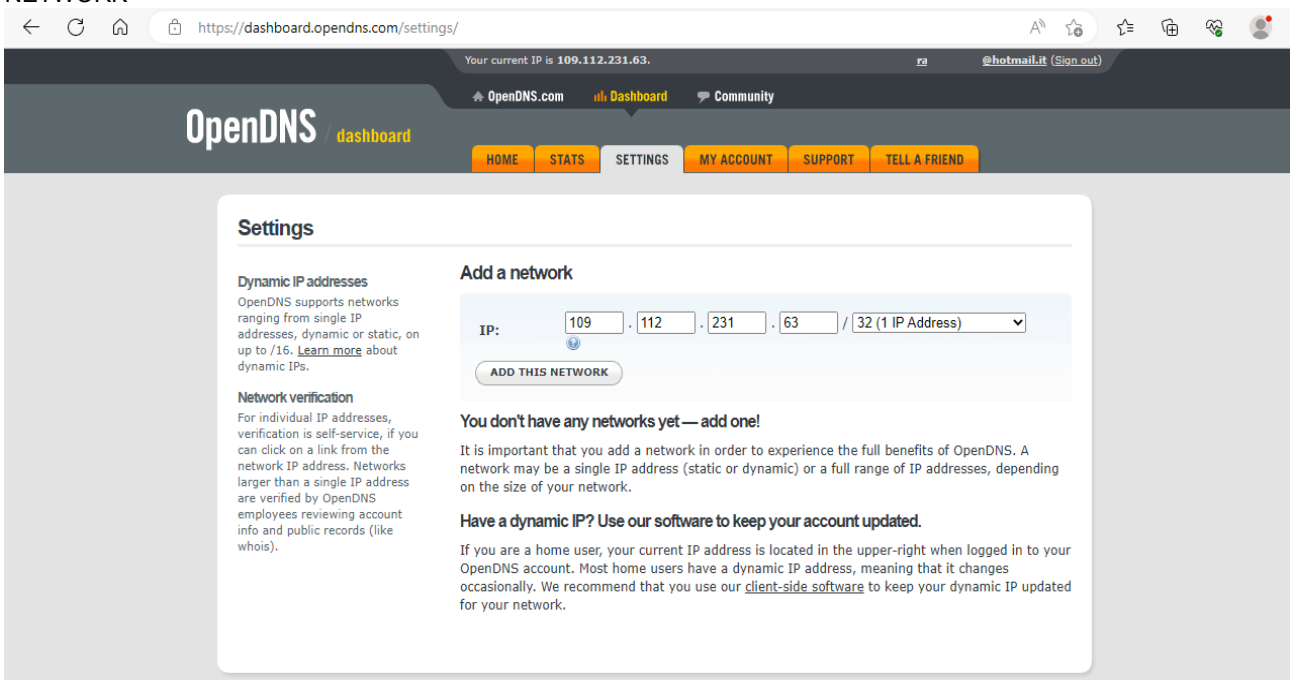
GET A FREE ACCOUNT

By clicking "Get A Free Account" you agree to the OpenDNS [Terms of Service](#) and [Privacy Policy](#)

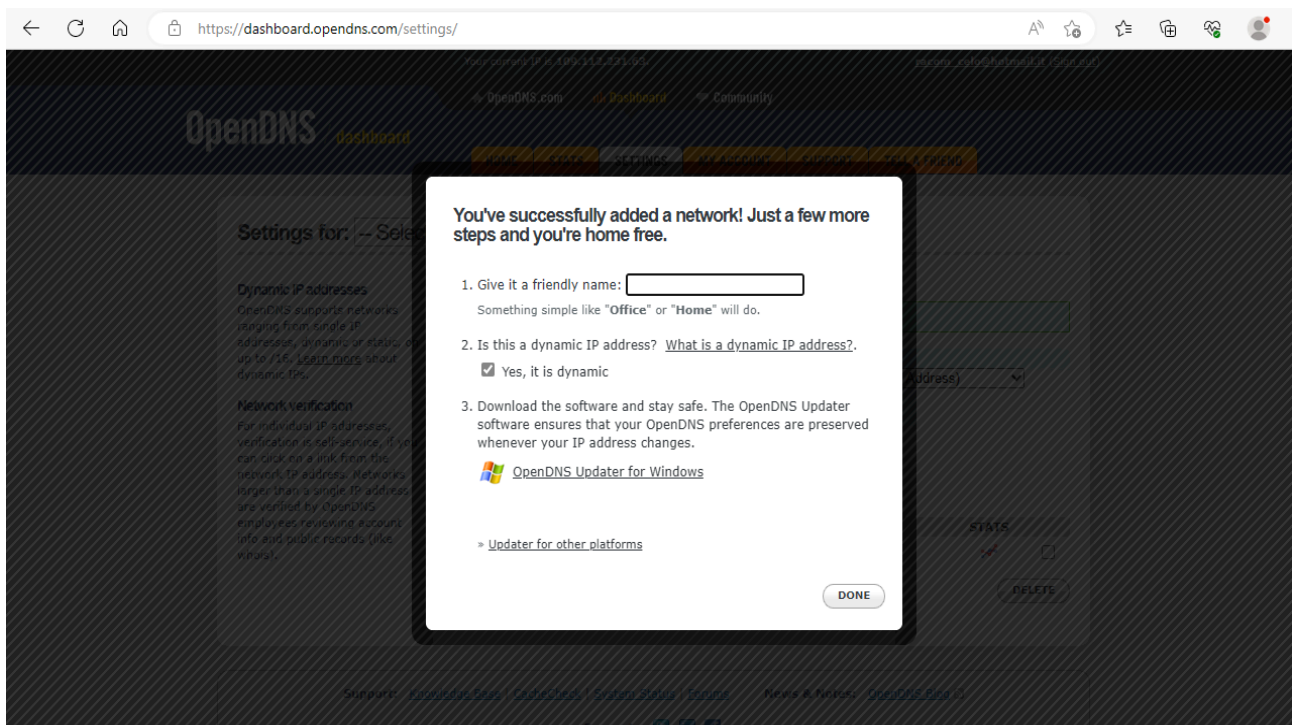
Accedere alla e-mail inserita durante la registrazione e confermare l'indirizzo e-mail collegandosi al link contenuto nell'e-mail di open DSN, e verrà aperta una pagina WEB dove sarà necessario selezionare ADD NETWORK



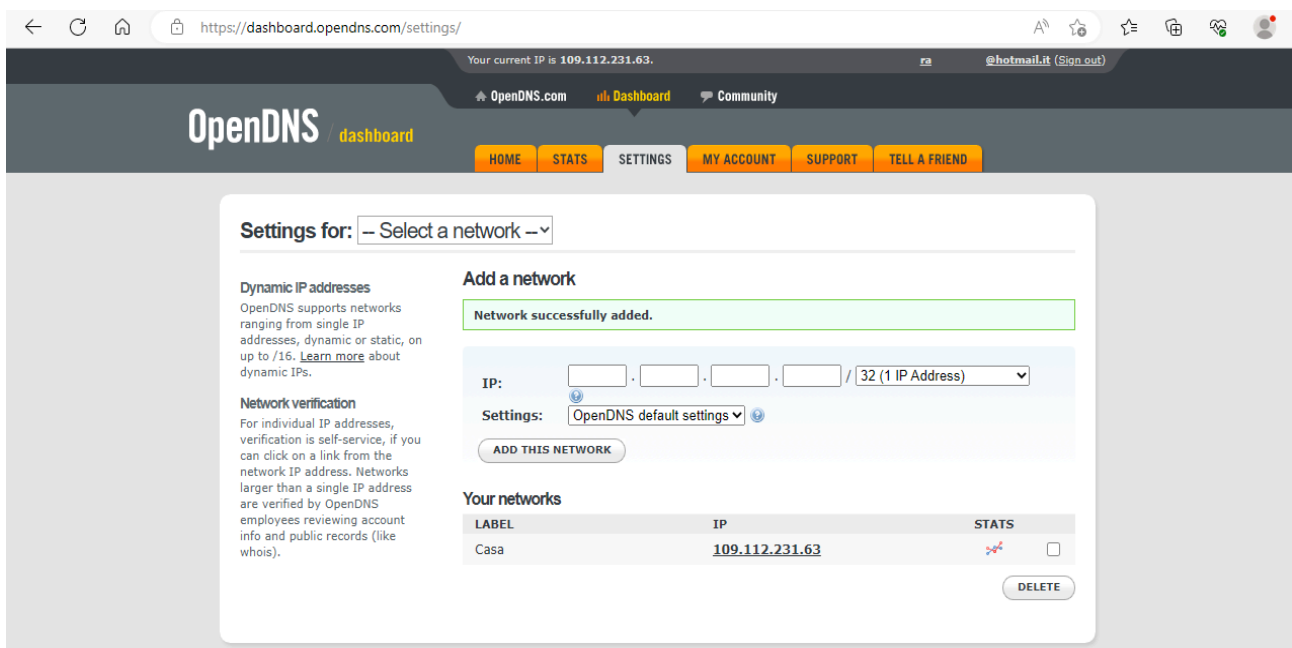
Nella pagina successiva il sistema rileva automaticamente l'indirizzo IP pubblico dell'utenza, è però necessario effettuare la procedura di attivazione collegandosi alla propria rete Etruriacom. Si prega di verificare che l'indirizzo IP rilevato sia coincidente con l'indirizzo IP comunicato da Etruriacom durante la richiesta di attivazione. Premere su "ADD THIS NETWORK"



Nella pagina successiva assegnare un nome a scelta per la propria utenza e premere il pulsante "DONE"

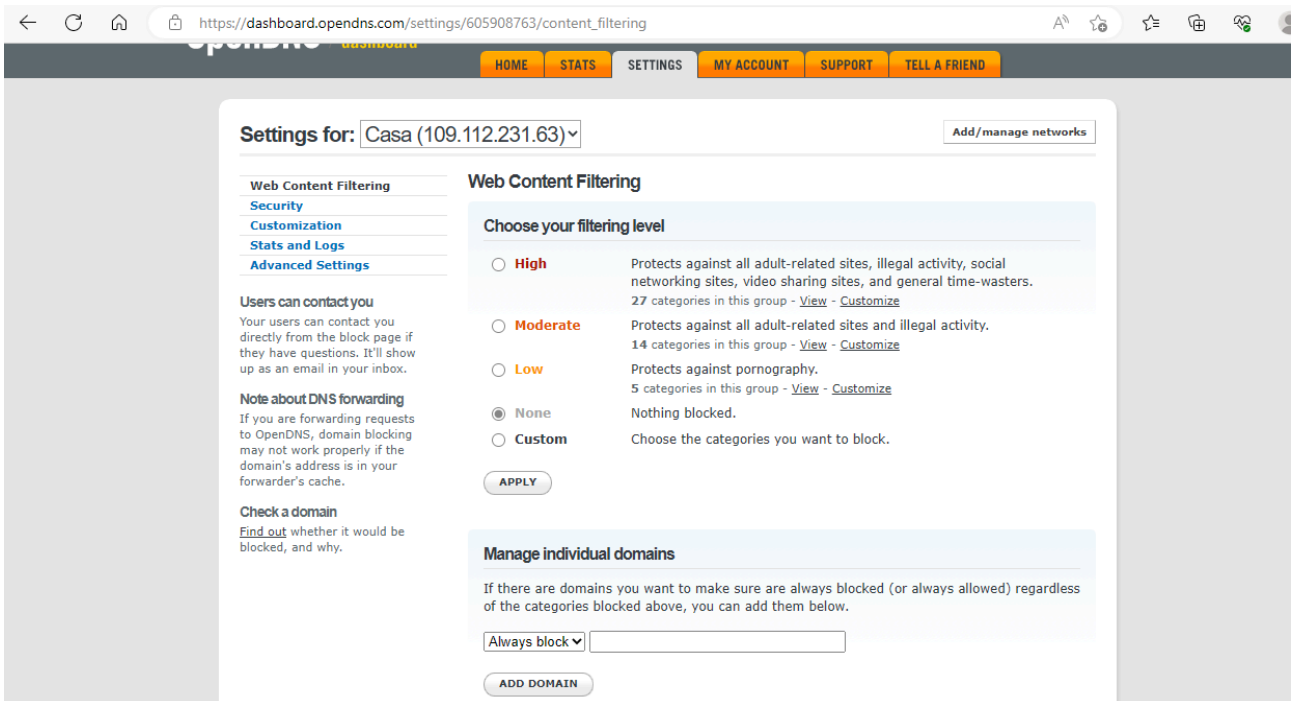


Un messaggio di conferma apparirà, a questo punto premere sull'indirizzo IP dell'utenza per accedere alle impostazioni.

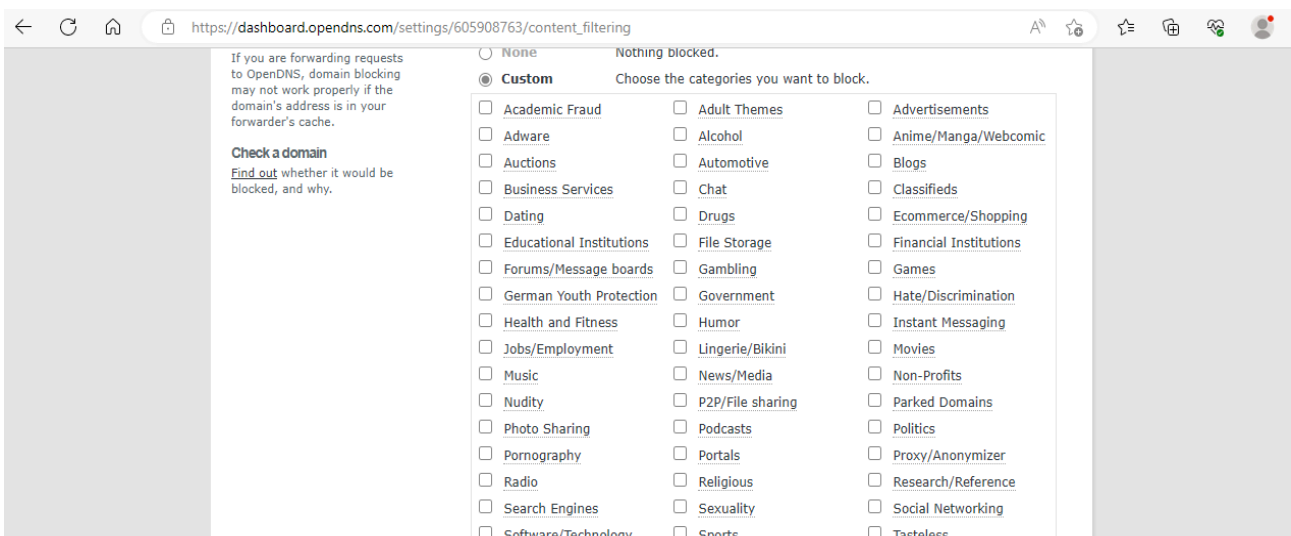


Nella pagina successiva sarà possibile selezionare il livello di protezione dal più basso al più elevato, e modificare le impostazioni di ogni livello.

Puoi anche specificare i siti internet che intendi bloccare, utilizzando la sezione **“manage individual domains”**, scrivendo l'URL del sito da bloccare esempio www.sitodabloccare.com e premendo il pulsante **“ADD DOMAIN”**



In alternativa selezionando il profilo **“CUSTOM”** è possibile selezionare e deselegionare a piacimento le varie categorie di blocco



Il servizio offre ulteriori possibilità di protezione come il blocco malware e phishing.



The screenshot shows the OpenDNS dashboard at the URL <https://dashboard.opendns.com/settings/605908763/security>. The page is titled "Impostazioni per: Casa (109.112.231.63)" and includes a navigation menu with "HOME", "STATS", "SETTINGS", "MY ACCOUNT", "SUPPORT", and "TELL A FRIEND". A sidebar on the left lists "Filtraggio dei contenuti Web", "Sicurezza", "Personalizzazione", "Statistiche e registri", and "Impostazioni avanzate". The main content area is under the "Sicurezza" section and contains three settings:

- Protezione da malware/botnet**: **Abilita la protezione di base da malware/botnet**
Quando vengono rilevate determinate botnet su scala Internet o colpi di malware particolarmente dannosi, offriamo protezione a tutti i nostri utenti in modo che il maggior numero di persone il più possibile può essere protetto dalla minaccia. In questo momento, questa funzione blocca il virus Conficker e Internet Explorer Zero Day Exploit, e viene continuamente ampliato per includere altri tipi di siti dannosi.
- Protezione dal phishing**: **Abilitare la protezione dal phishing**
Abilitando la protezione dal phishing, proteggerai Tutti gli utenti della tua rete da siti di phishing noti utilizzando i migliori dati disponibili.
- Risposte sospette**: **Blocca indirizzi IP interni**
Se abilitate, le risposte DNS contenenti indirizzi IP elencati in [RFC1918](#) verranno filtrati. Ciò consente di prevenire [gli attacchi di rebinding DNS](#). Ad esempio, se badstuff.attacker.com punta a 192.168.1.1, Questa opzione filtrerebbe la risposta.

Verificare il funzionamento: dopo aver configurato il servizio, è consigliabile verificare il suo funzionamento visitando alcuni siti web per testare la corretta attivazione dei filtri. Nota che per l'applicazione del filtro e le eventuali future modifiche potrebbero essere necessari dai 10 ai 15 minuti.

Ricordati di salvare il link per accedere alle impostazioni e monitoraggio del Parental control, e di conservare e non divulgare le credenziali di accesso.

In caso di perdita delle credenziali è possibile recuperarle effettuando la procedura guidata al link: <https://login.opendns.com/reset>