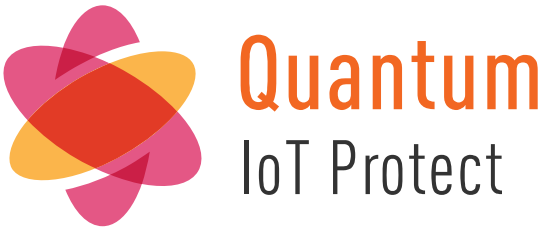
HOW TO – QUANTUM IOT PROTECT – ONBOARDING



Documento escrito por: Lisandro Weissheimer da Silva
Security Engineering Brazil
Dezembro/2023

CONTEÚDO

Sobre a solução: Quantum IoT Protect

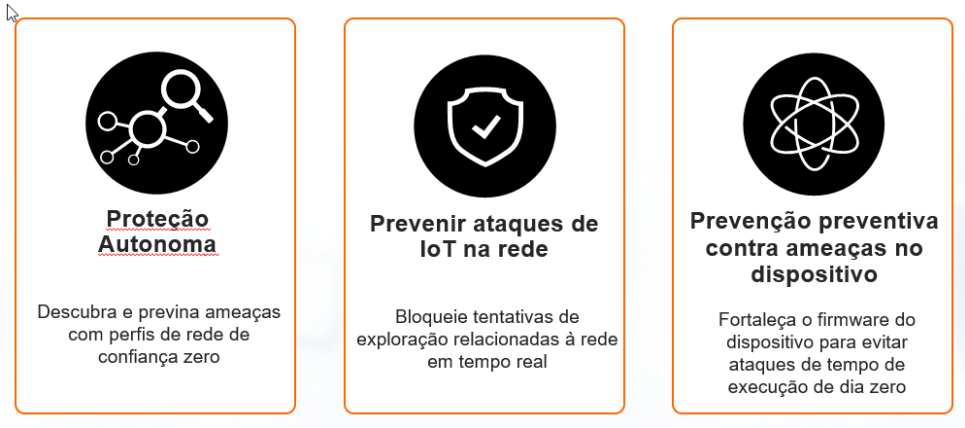
Cenário atual

O uso de dispositivos da Internet das Coisas (IoT) em aplicações empresariais, de saúde e industriais oferece benefícios de produtividade, mas também expõe as redes à ameaças cibernéticas em constante evolução.

De câmeras IP e elevadores inteligentes a dispositivos médicos e controladores industriais, o Quantum IoT Protect protege suas redes IoT contra ataques cibernéticos.

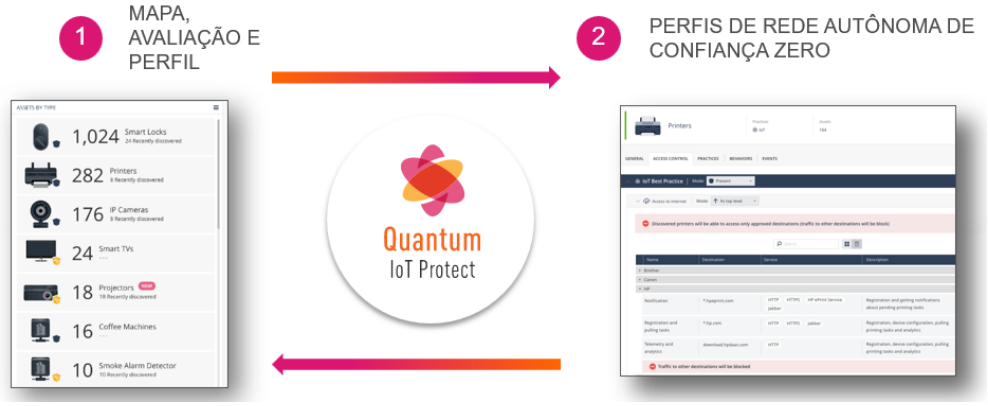
Quantum IoT Protect

Prevenção autônoma de ameaças para proteção de rede e no dispositivo



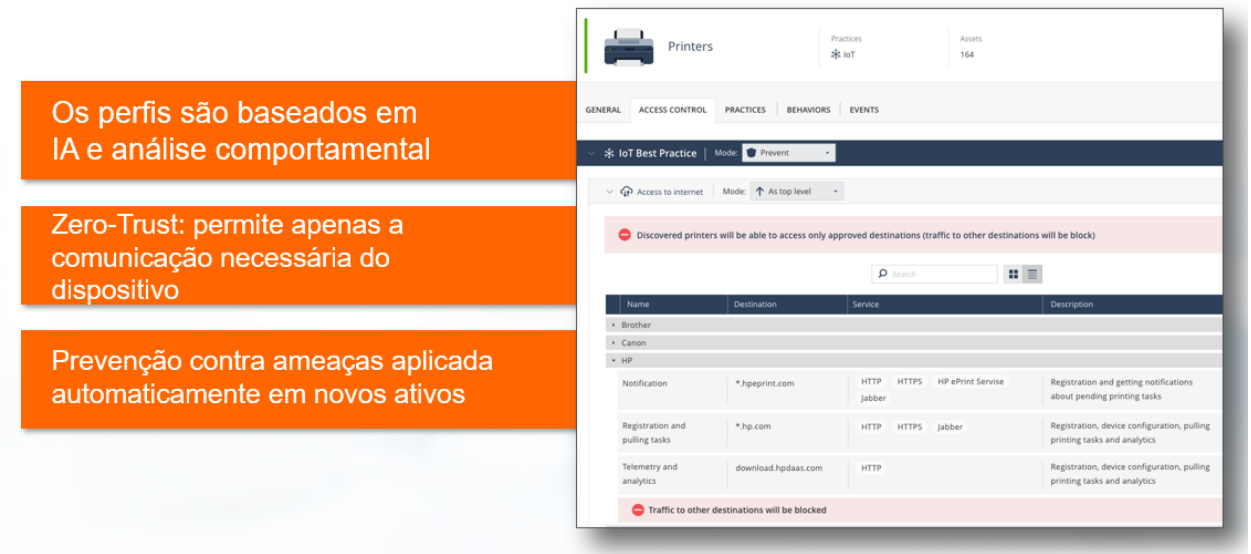
Proteção Autonoma para dispositivos IoT

Mais de 200 perfis autônomos por tipo de dispositivo, categoria e fornecedor

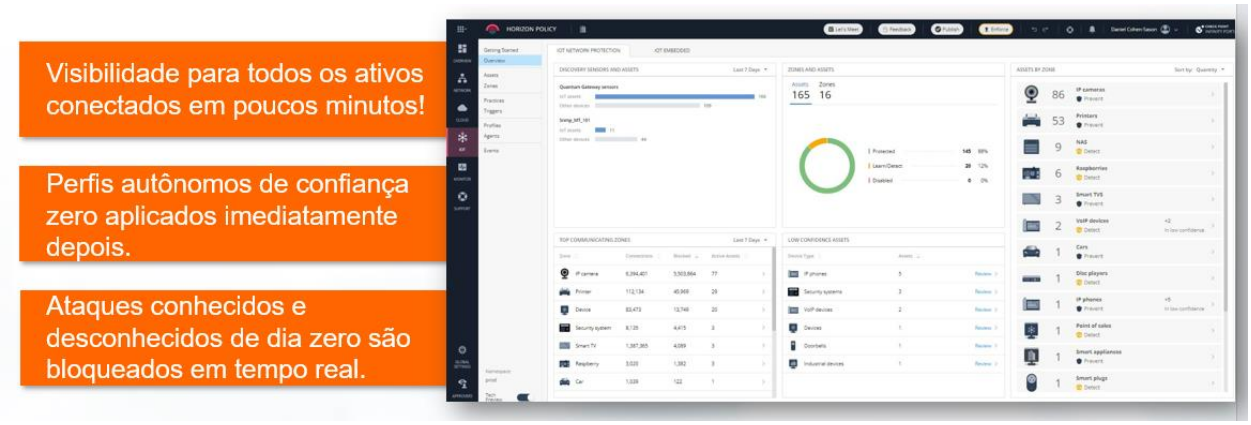


Perfis de rede IoT autônoma de confiança zero

Com o Quantum IoT Protect, você também começa a entender como os dispositivos estão se comunicando e com o que estão se comunicando. Aproveitamos técnicas de IA e aprendizado de máquina para compreender completamente os padrões e criar automaticamente regras que permitem a comunicação adequada para o dispositivo e bloquear qualquer ação não autorizada que possa servir como uma ameaça potencial à rede. É aqui que você realmente percebe a peça de prevenção.



Gerenciamento simples de IoT em um único console



Uma solução abrangente de segurança de IoT é necessária para proteger sua empresa contra esses riscos e é um componente vital da estratégia de segurança cibernética de cada empresa.

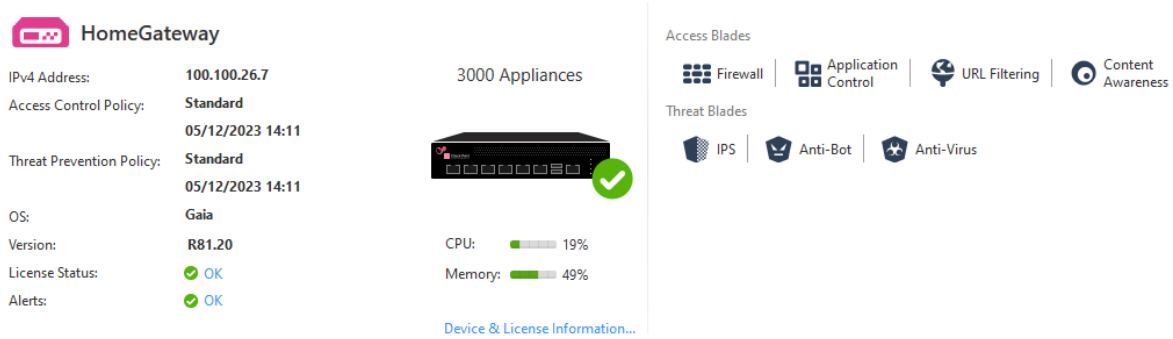
Onboarding do Quantum IoT Protect

Cenário utilizado

Os próximos passos descrevem o processo de onboarding do Quantum IoT Protect bem como as características do ambiente utilizado. Neste cenário presuminos que o gateway de segurança já está operacional e sua manager devidamente conectada e ativada. Este exemplo utiliza a manager SaaS Smart-1 Cloud e o procedimento leva isto em conta.

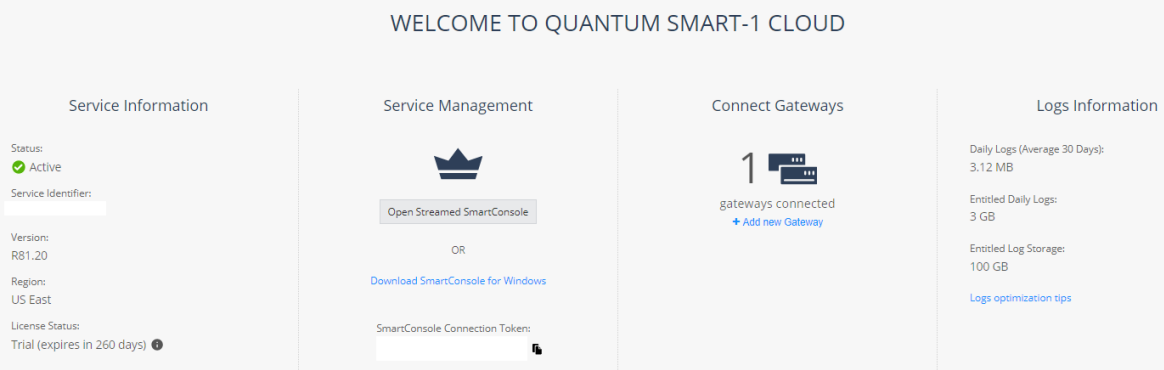
Gateway

Modelo: 3600
Versão Gaia: R81.20 Jumbo Hotfix Take 41
Kernel: 3.10.0-1160.15.2cpx86_64
Edition: 64-bit
Build: 631



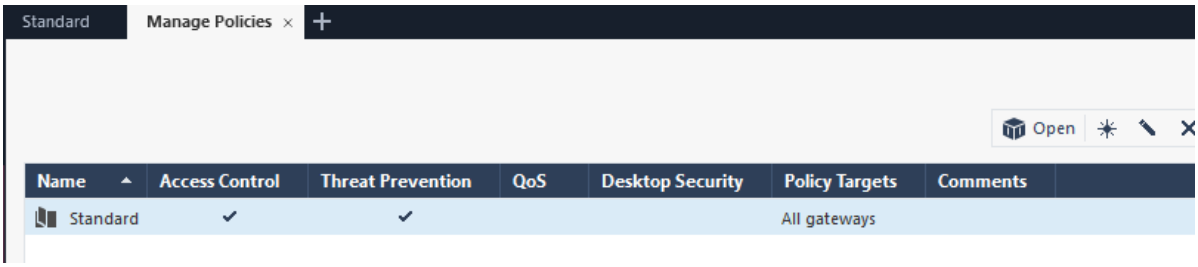
Manager

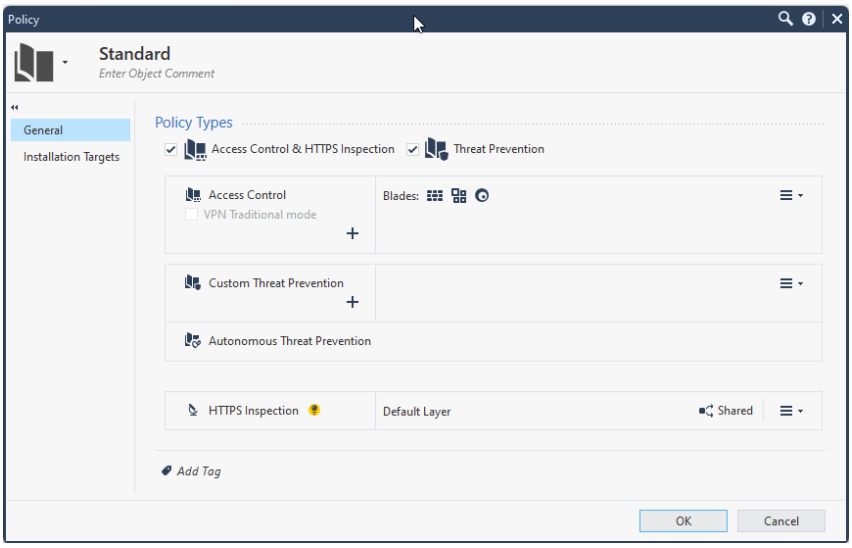
Modelo: Smart-1 Cloud



Políticas

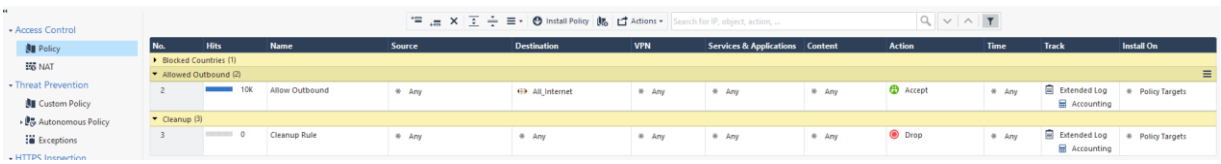
Abaixo temos as políticas criadas, onde podemos notar que há apenas a layer de Controle de Acesso, no pacote de políticas Standard.





Regras de Acesso

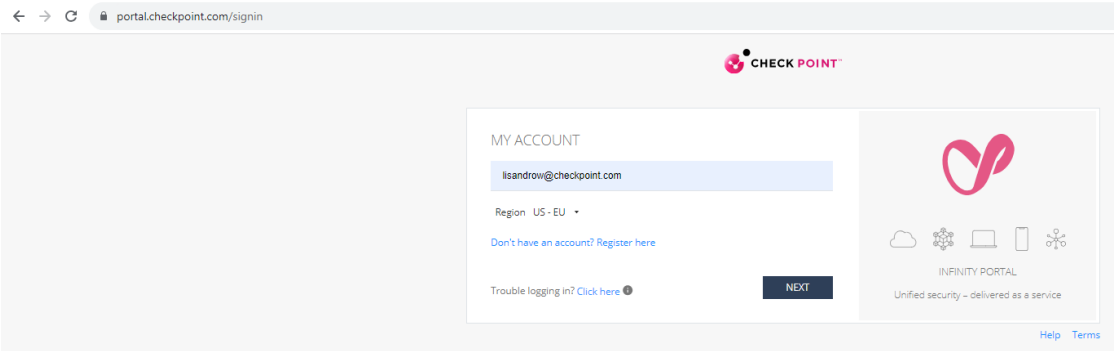
As regras de acesso criadas bloqueiam acesso inboud de determinados países. Esta regra não é mandatória, mas recomenda-se como boa prática. Possui ainda uma regra que permite qualquer tráfego de saída para a Internet e uma regra de Cleanup.



Ativação do serviço IoT Protect no Portal Infinity

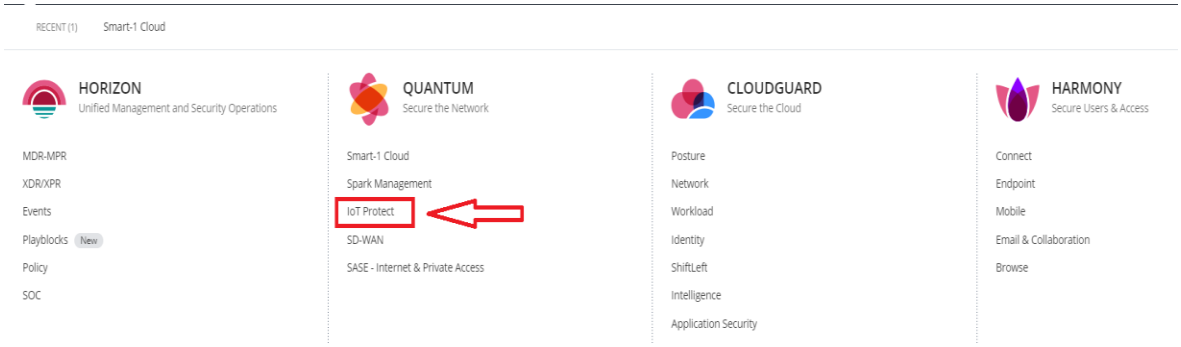
Para este exemplo iremos considerar que você já tem uma conta criada no Portal Infinity e sua instância de gerência, Smart-1 Cloud, está ativa e funcional, como mostrado nas imagens anteriores.

1- Faça login no Portal Infinity (https://portal.checkpoint.com) com uma conta que possua direitos adminitrativos e pode ativar novos serviços:

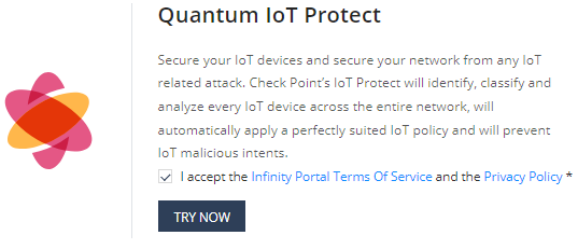


2- Após o login, vá até o canto superior esquerdo e clique no ícone do menu:

3- Selecione IoT Protect, como mostra a imagem abaixo:

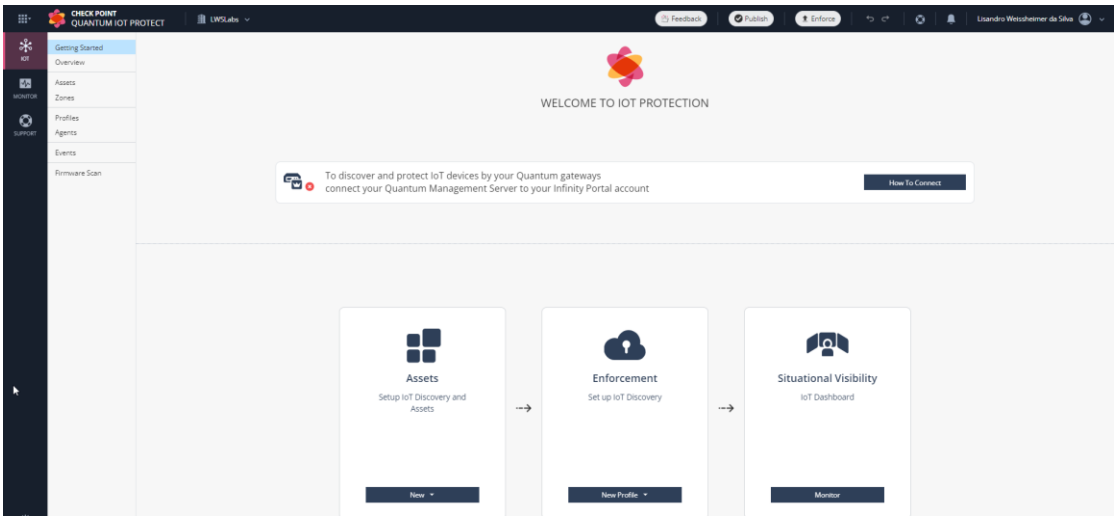


4- Aceite os termos e clique em TRY NOW:

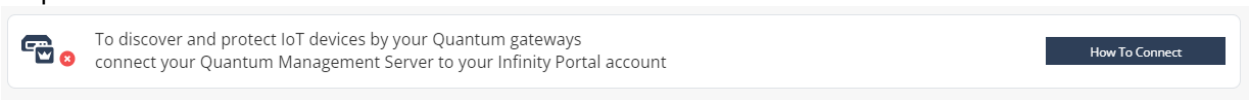


5- Aguarde a ativação dos serviços:

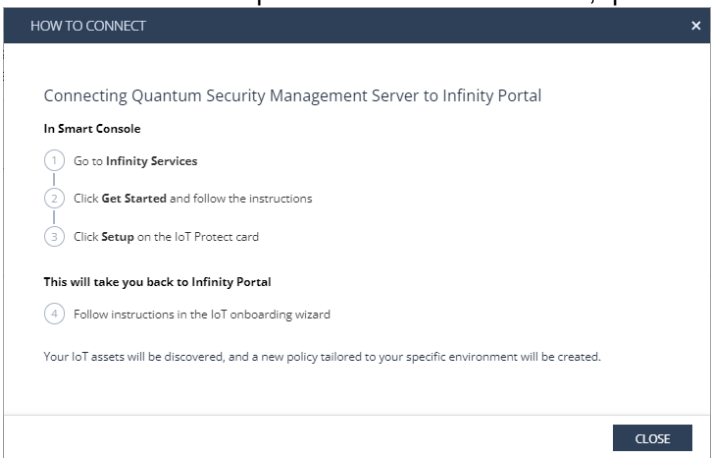
6- Após a ativação dos serviços, é necessário realizar algumas configurações na Smart-1 Cloud. A tela abaixo indica que os serviços foram ativados mas ainda dependem de configurações para funcionarem corretamente:



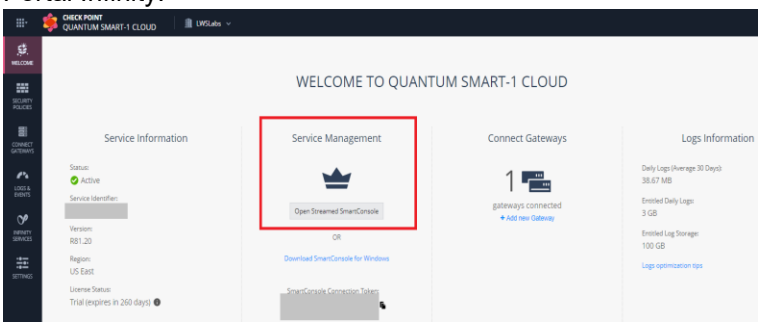
7- Clique em How To Connect:



8- A tela exibida traz os passos a serem executados, que faremos na sequencia:

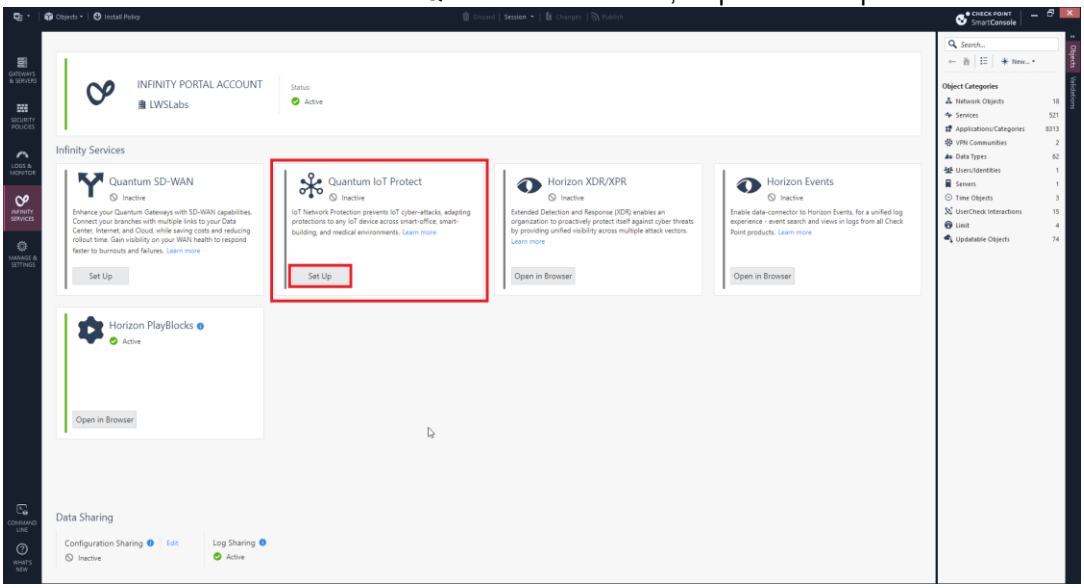


9- Acesse a SmartConsole instalada em seu computador ou através da Streamed SmartConsole no Portal Infinity:

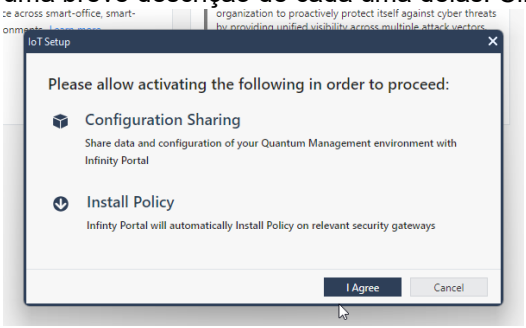


10- Neste exemplo usaremos a SmartConsole instalada localmente. Clique no botão Infinity Services:

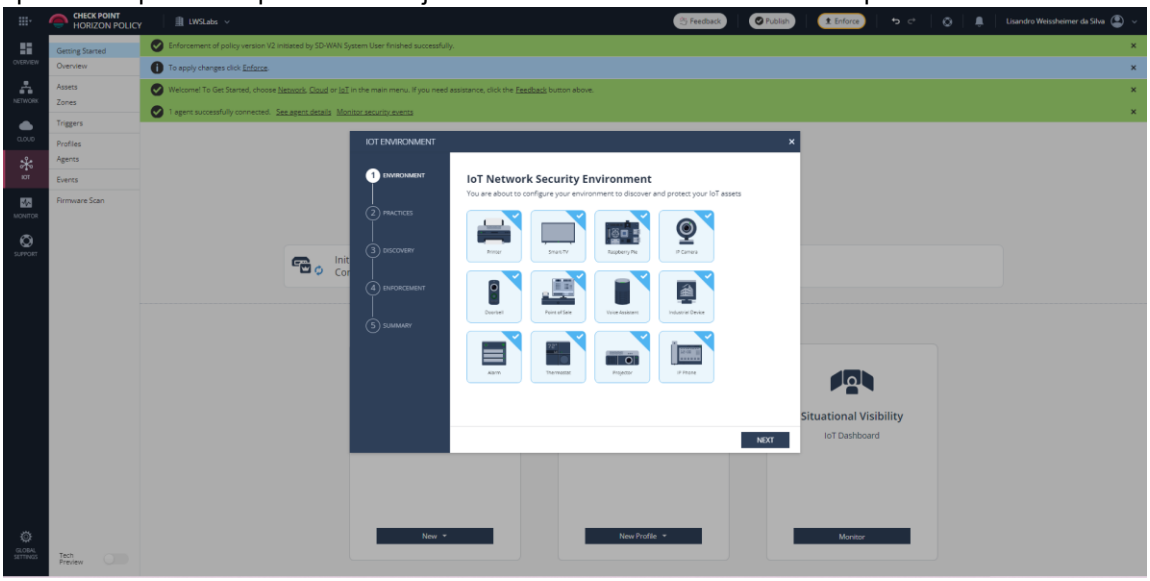
11- A tela abaixo será exibida. No card Quantum IoT Protect, clique em Setup:



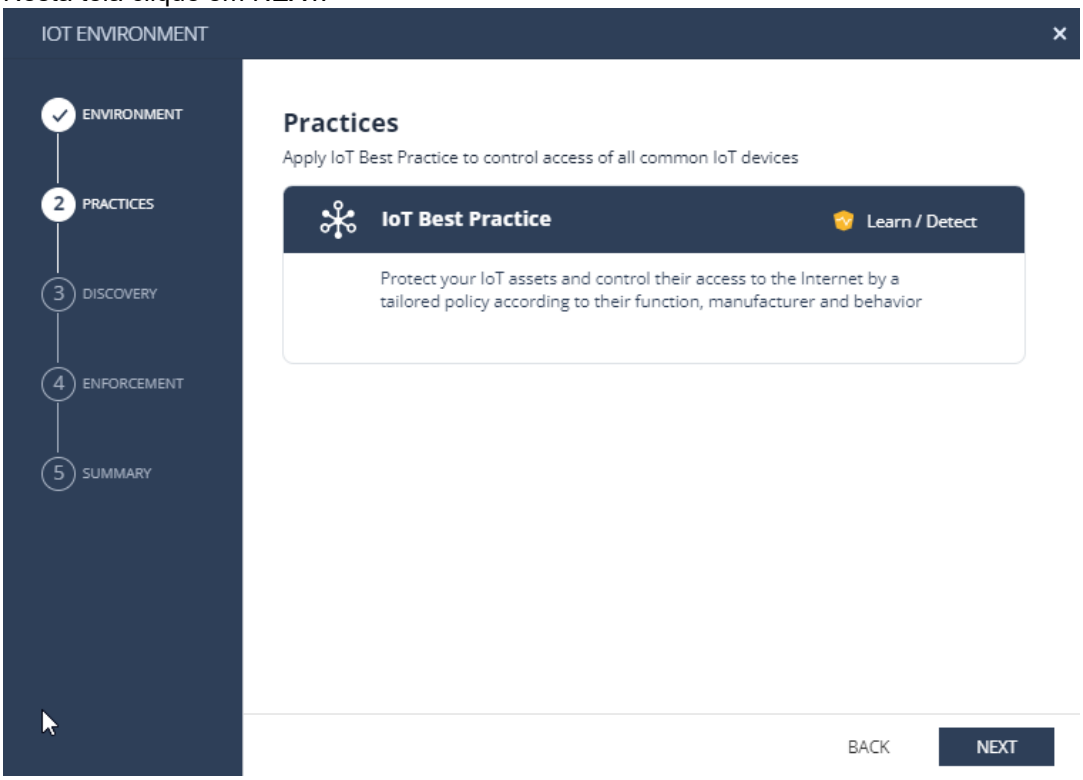
12- A tela abaixo traz as duas ações a serem executadas, Configuration Sharing e Install Policy, e uma breve descrição de cada uma delas. Clique em I Agree



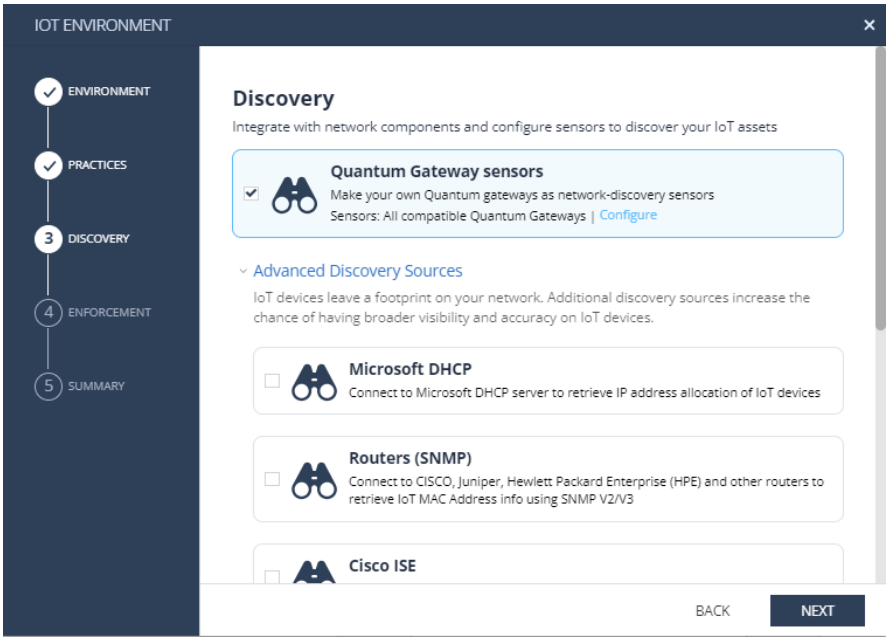
13- Você será direcionado ao Portal Infinity para finalizar a configuração. Certifique-se que todos os tipos de dispositivos que você deseja identificar estão selecionados e clique em NEXT:



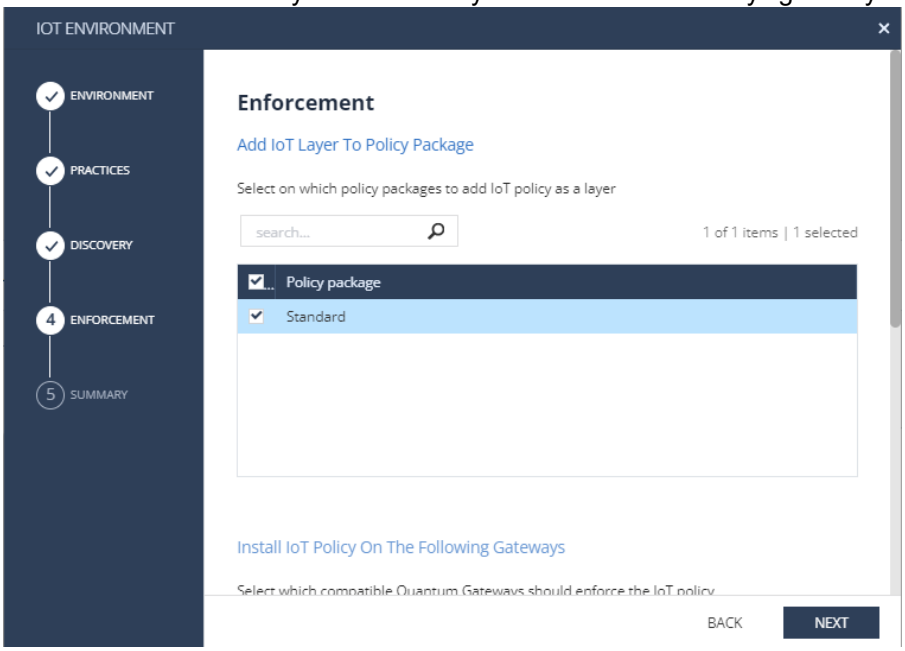
14- Nesta tela clique em NEXT:

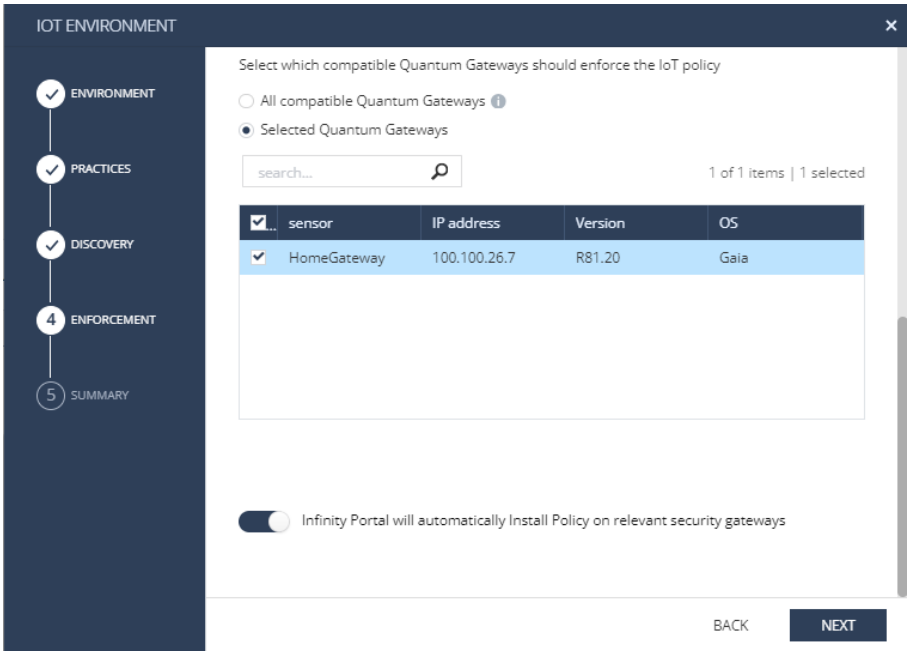


15- Na tela abaixo, Discovery, selecione apenas Quantum Gateway sensors, se ainda não estiver marcado. Note que outras fontes podem ser utilizadas para descoberta. Não trataremos destas outras fontes neste documento, nosso foco é ativar os serviços de descoberta e proteção nos Gateways de Segurança Check Point:

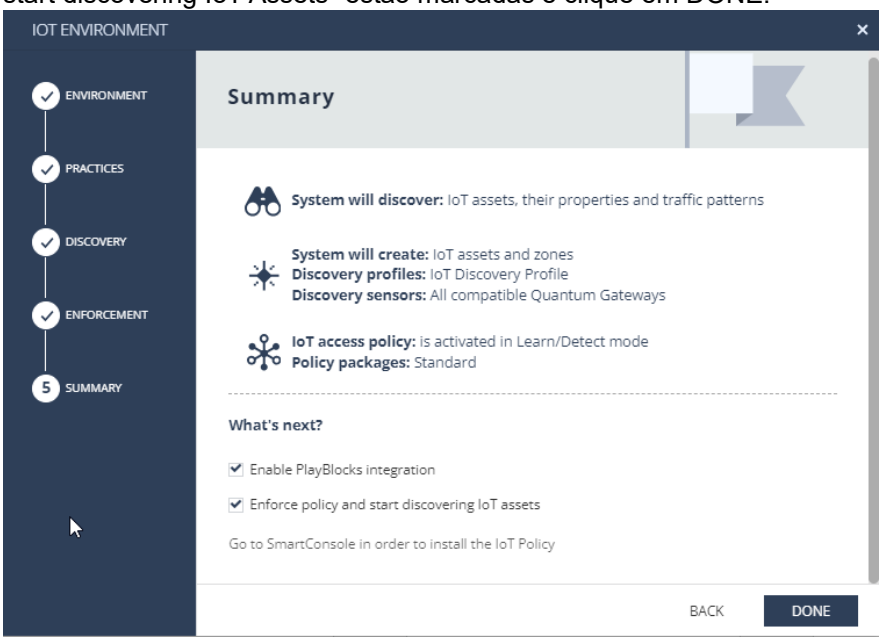


16- Selecione a política onde serão adicionadas as regras de acesso e proteção para IoT. Após selecionar a politica, role a tela para baixo e escolha em quais Gateways você terá a layer de IoT e não equeça de marcar a última opção, abaixo dos Gateways selecionados, onde diz “Infintiy Portal will automatically Install Policy on relevant security gateways”. Clique em NEXT.

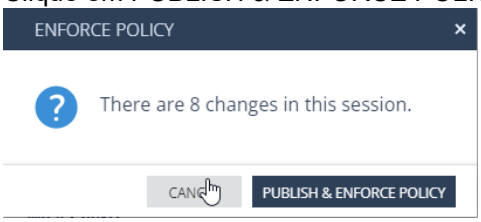




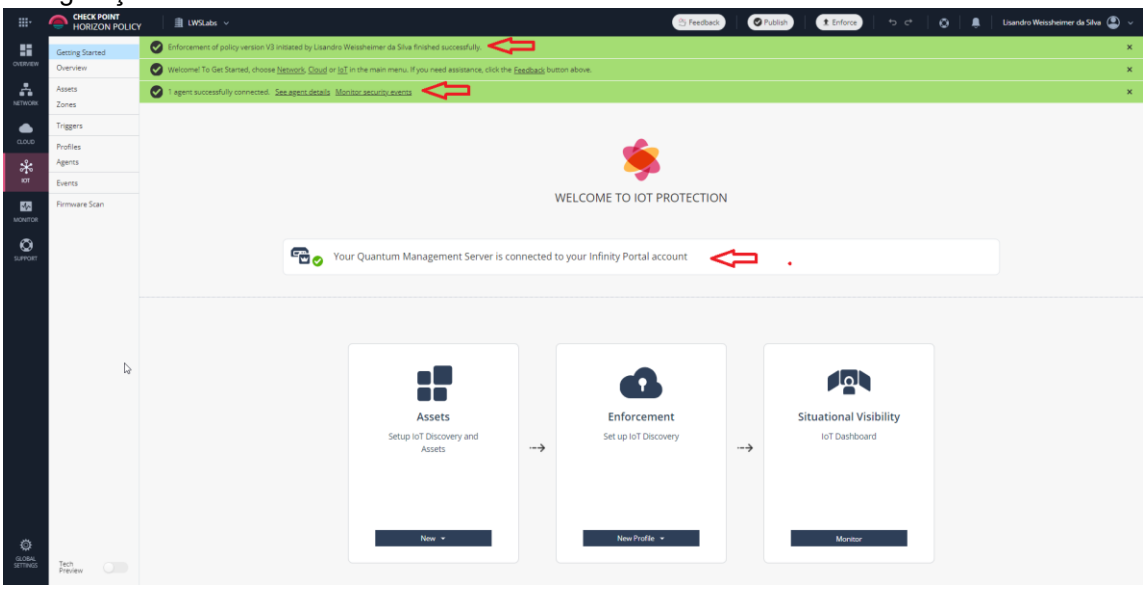
17- Na tela final, certifique-se que as opções “Enable PlayBlocks Integration” e “Enforce policy and start discovering IoT Assets” estão marcadas e clique em DONE:



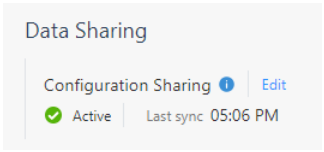
18- Será exibida a mensagem abaixo, indicando quantas alterações foram feitas nesta sessão. Clique em PUBLISH & ENFORCE POLICY:

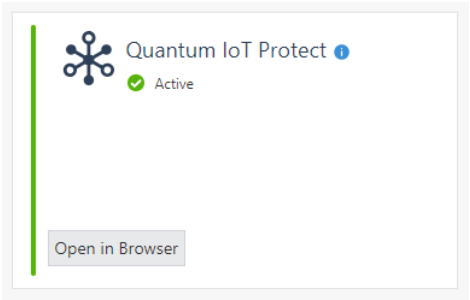


19- Ao término do enforce, você será direcionado para este tela, indicando que houve sucesso na configuração:

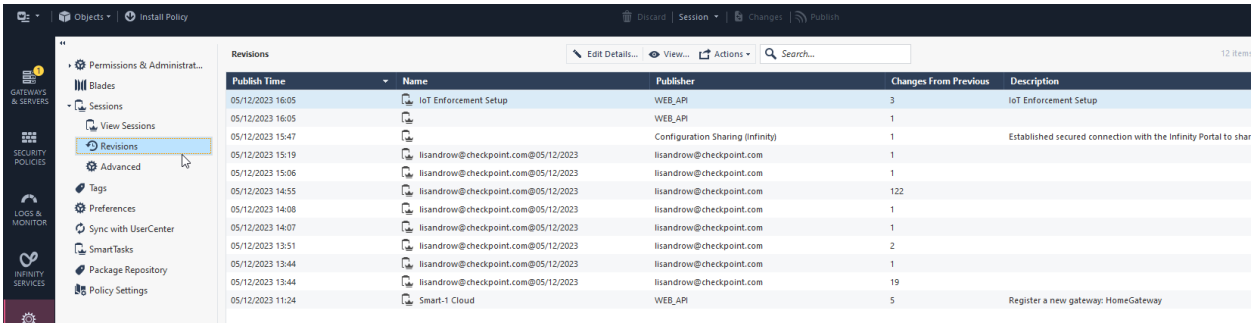


20- Retorne a SmartConsole no item Infinity Services e verifique se a opção Configuration Sharing está ativa e se o card do Quantum IoT Protect está ativo também:

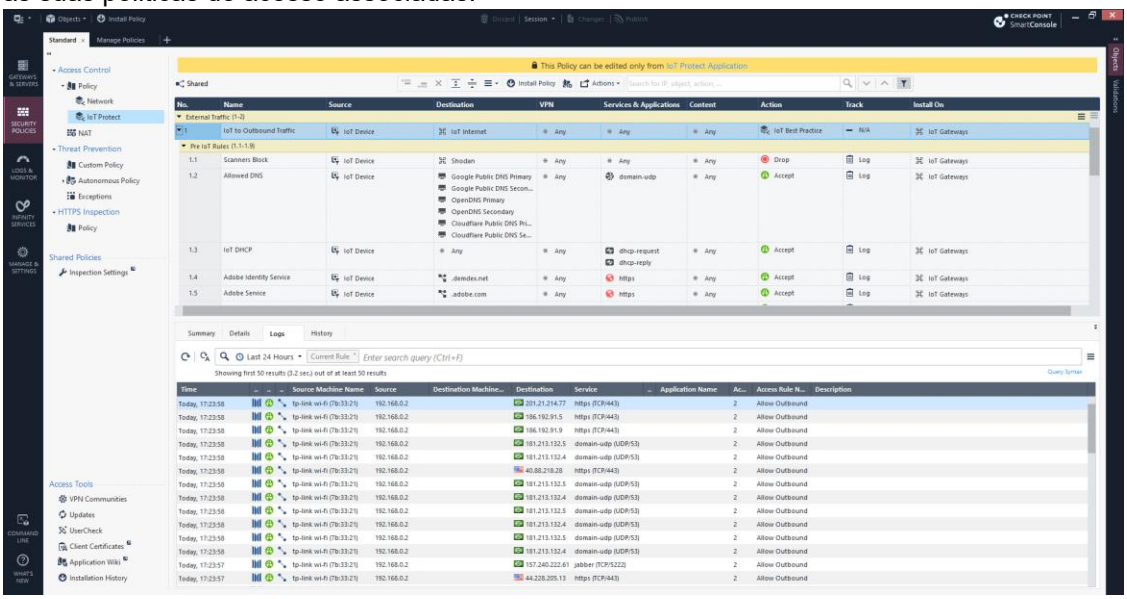




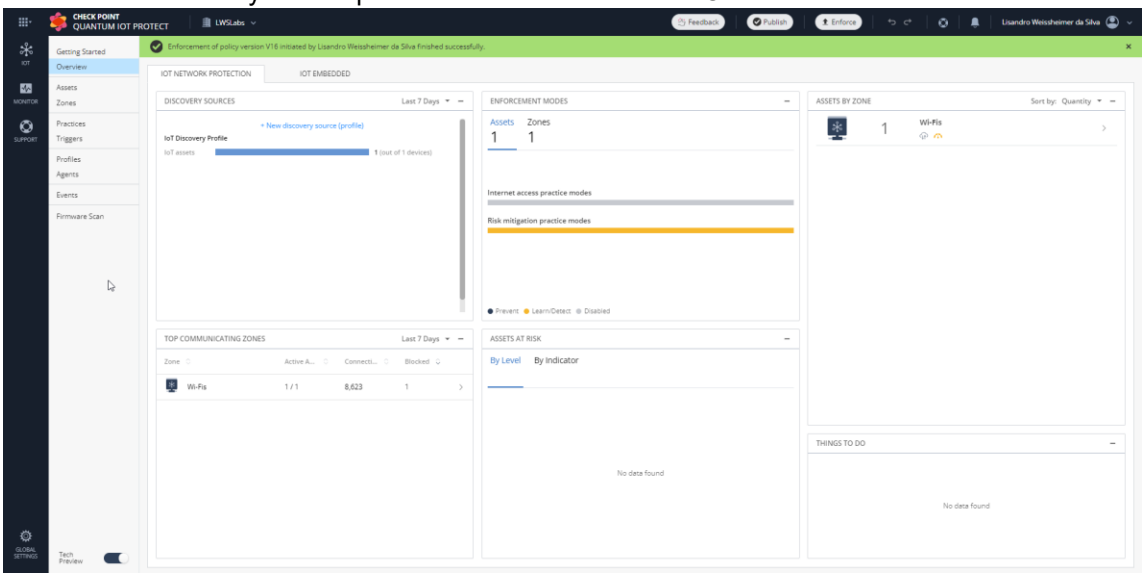
21- Na SmartConsole, vá em MANAGE & SETTINGS e selecione Sessions e depois Revisions. Deve haver uma sessão de enforcement do IoT, como abaixo:



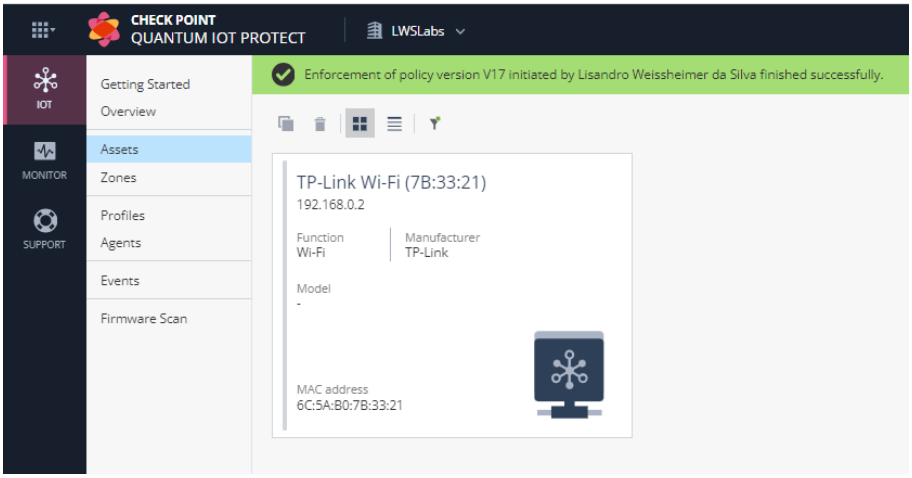
22- Na aba SECURITY POLICIES da SmartConsole você deve encontrar agora a layer IoT Protect e as suas politicas de acesso associadas:



23- Volte ao Portal Infinity e verifique se existem dados na aba Overview:



24- Na aba Assets você terá a lista dos ativos descobertos até o momento:



Deste ponto em frente, novos ativos serão descobertos e adicionados ao Quantum IoT Protect.

Para saber mais sobre Quantum IoT Protect, clique aqui.

Para saber mais sobre Smart-1 Cloud, clique aqui.