

Cisco IQ Link Release Notes v1.2.0

Inleiding

Cisco IQ™ biedt klanten verbeteringen en functies die zijn ontworpen om de zichtbaarheid van bedrijfsmiddelen te verbeteren, slimmere inzichten te bieden in hun omgevingen en het beheer van casussen te stroomlijnen. Daarnaast optimaliseren AI-functies zoals de AI Assistant de operationele resultaten en de Cisco IQ-gebruikerservaring door contextueel inzicht te bieden dat gebruikers in staat stelt proactieve, geïnformeerde beslissingen te nemen en processen voor klantbetrokkenheid en succes te stroomlijnen.

Cisco IQ Link verzamelt en verzendt veilig asset telemetrie van uw on-premises netwerk naar Cisco IQ, waardoor AI-aangedreven voorspellende inzichten u helpen de zichtbaarheid van het netwerk te verbeteren, problemen te anticiperen en operationele efficiëntie te stimuleren.

Dit document schetst nieuwe functies en bekende problemen voor Cisco IQ Link v1.2.0.

Belangrijkste kenmerken

Deze versie introduceert de volgende nieuwe functies.

Ondersteuning voor nieuwe apparaatverzameling

De Cisco IQ Connector ondersteunt nu verbeterde mogelijkheden voor apparaatdetectie.

CDP- en LLDP-detectie

Hiermee kunt u apparaten opsporen met Cisco Discovery Protocol (CDP)- en Link Layer Discovery Protocol (LLDP)-protocollen vanaf een seed-apparaat.

IP Range Discovery

Cisco IQ Connector maakt het nu mogelijk om apparaten binnen een bepaald IP-adresbereik te scannen.

Scannen met Bestand uploaden

Gebruikers kunnen bestanden uploaden met meerdere IP-bereiken en meerdere CDP- en LLDP-ingangen om automatisch apparaatdetectie uit te voeren.

Verbeteringen in gebruikersbeheer

De volgende verbeteringen zijn bedoeld om de authenticatie- en beheerprocessen van gebruikers te vereenvoudigen en gebruikers binnen het systeem een betere controle en beveiliging te bieden.

Microsoft Entra IDP SSO

Cisco IQ Link ondersteunt nu Microsoft Entra ID (voorheen Azure AD) als Identity Provider (IDP) voor naadloze Single Sign-On (SSO)-mogelijkheden, waardoor organisaties hun bestaande Entra ID-infrastructuur kunnen gebruiken voor gecentraliseerde authenticatie. Deze functie verbetert de beveiliging door gebruik te maken van bestaande Multi-Factor Authentication (MFA) en voorwaardelijke toegangsbeleid.

Lokaal gebruikersbeheer

Gebruikers kunnen meerdere gebruikers veilig aan boord hebben en beheren met verschillende toegangsrechten. Lokale gebruikers die door een beheerder zijn gemaakt, kunnen de optie "Aanmelden" gebruiken tijdens hun eerste aanmelding en veilig hun eigen wachtwoorden instellen met behulp van het e-mailadres dat door de beheerder is geconfigureerd.

Self-service beveiligingsbeheer

U kunt nu lokale beveiligingsinstellingen onafhankelijk beheren en controle over accounttoegang en herstel bieden. Self-service mogelijkheden omvatten de mogelijkheid om vergeten wachtwoorden opnieuw in te stellen en beveiligingsvragen te configureren, waardoor een meer gestroomlijnde en veilige gebruikerservaring mogelijk is zonder externe ondersteuning.

Configureerbare inlogbanner

Om de naleving van de best practices op het gebied van beveiliging te ondersteunen, biedt Cisco IQ Link nu een configureerbare aanmeldingsbannerfunctie waarmee accountbeheerders verplichte systeemmeldingen en beveiligingswaarschuwingen op het aanmeldingsscherm kunnen weergeven. Banners zijn volledig aanpasbaar en kunnen worden ingesteld om expliciete

gebruikersbevestiging te vereisen voordat u zich aanmeldt.

Bekende problemen

De volgende problemen worden actief aangepakt in Cisco IQ Link.

Veld Terugkerende planning geeft UNIX Cron-syntaxis weer

Momenteel vereist de terugkerende planninginvoer voor het uploaden van netwerkscanbestanden een UNIX-cron-expressie met vijf (5) velden (bijvoorbeeld 0 2 * * *). Gebruikers die niet bekend zijn met de cron syntax vinden dit invoerformaat mogelijk onduidelijk. Gebruikers kunnen echter online meer gedetailleerde informatie krijgen over cron syntax en voorbeelden.

Adresbeperking Syslog-server

Momenteel moet de Syslog-server worden opgegeven als een IP-adres en niet als een volledig gekwalificeerde domeinnaam (FQDN).

Proxyverificatie Speciale tekenbeperking

Momenteel ondersteunen proxyverificatiereferenties geen speciale tekens. Het gebruik van speciale tekens in de proxy-gebruikersnaam of het wachtwoord kan communicatieproblemen veroorzaken tussen Cisco IQ Link en Cisco IQ.

Problemen opgelost

De volgende problemen zijn opgelost als onderdeel van de v1.2.0-release.

Wachtwoordsynchronisatie

Voorheen kon het bijwerken van het wachtwoord van de lokale beheerder via de Cisco IQ Link UI (onder Beveiligingsinstellingen voor Lokale beheerder) niet worden gesynchroniseerd met de toegang tot de VM SSH, wat tot verificatiefouten leidde. Dit probleem is opgelost en gebruikers kunnen nu hun referenties bijwerken via de gebruikersinterface zonder handmatige tussenkomst of extra ondersteuning om authenticatieconflicten op te lossen.

Fouten in API-snelheidslimiet tijdens gegevensverzameling

Voorheen kon Cisco IQ Link soms de volledige apparaatdataset niet verzamelen wanneer de aanvraagvolumes de API-snelheidslimieten van Catalyst Center overschreden, wat resulteerde in een fout "API-snelheidslimiet overschreden". Dit probleem is opgelost; het gegevensverzamelingsproces is geoptimaliseerd om verzoeken efficiënter te beheren, deze fouten te voorkomen en een consistente gegevensverzameling te garanderen.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.