Configuration de l'authentification SSO (Single Sign-On) avec Cisco Cloud Sign-On

Table des matières

Problème

Lors de la migration d'Umbrella vers Secure Cloud Control, le comportement de l'authentification unique (SSO) administrative a changé de manière inattendue. Au lieu d'utiliser l'ID Microsoft Entra précédemment configuré pour l'authentification et l'AMF, les administrateurs devaient s'authentifier à l'aide de la connexion Cisco Cloud avec DUO. Les administrateurs ont donc été invités à définir de nouveaux mots de passe et à s'inscrire à DUO pour l'authentification multifacteur.

Environnement

- Technologie : Accès sécurisé (anciennement Umbrella)
- Migration : Un parapluie pour un contrôle cloud sécurisé
- Authentification: Microsoft Entra ID (Azure AD) configuré en tant que fournisseur d'identité
- Multi-Factor Authentication : Microsoft 365 MFA précédemment configuré
- Nouvelle méthode d'authentification : Connexion à Cisco Cloud avec DUO

Résolution

La migration de l'authentification de Microsoft Entra ID vers Cisco Cloud Sign-on est une étape obligatoire qui se produit pendant le processus de migration Secure Access. Les étapes suivantes doivent être suivies pour configurer correctement l'authentification de l'interface utilisateur SAML :

Étape 1: Terminer la migration d'accès sécurisé

Effectuez la migration complète de Secure Access avant d'essayer de configurer l'authentification

de l'interface utilisateur SAML dans Secure Access. Cela garantit que tous les composants sont correctement migrés et prêts pour la configuration de l'authentification.

Étape 2: Configurer l'authentification SAML via le contrôle cloud de sécurité

La configuration de l'authentification de l'interface utilisateur SAML est désormais gérée via l'interface SCC (Security Cloud Control) plutôt que directement dans Secure Access. Accédez à Security Cloud Control > Authentication Settings pour accéder aux options de configuration du fournisseur d'identité.

Étape 3: Vérifier la configuration du fournisseur d'identités

Vérifiez et validez la configuration du fournisseur d'identités dans la page Security Cloud Control. Assurez-vous que l'intégration Microsoft Entra ID est correctement configurée pour le nouvel environnement.

Motif

Le changement de comportement d'authentification fait partie du processus de migration obligatoire d'Umbrella vers Secure Access. Au cours de cette migration, l'authentification SAML passe automatiquement de Microsoft Entra ID à Cisco Cloud Sign-on, ce qui nécessite DUO pour l'authentification multifacteur. Il s'agit d'une modification architecturale requise dans la nouvelle plate-forme d'accès sécurisé où les paramètres d'authentification sont gérés de manière centralisée via le contrôle cloud de sécurité plutôt qu'au sein des interfaces de produit individuelles.

Autres informations utiles

- Intégration des fournisseurs d'identités
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.