



Exploiter la distribution des politiques SCCM

Extraction d'identifiants via configurations permissives et relai d'authentification

SSTIC 2025

06/06/2025



Quentin Roland

Pentester

Les politiques SCCM : contexte et concepts

Les politiques SCCM : contexte et concepts

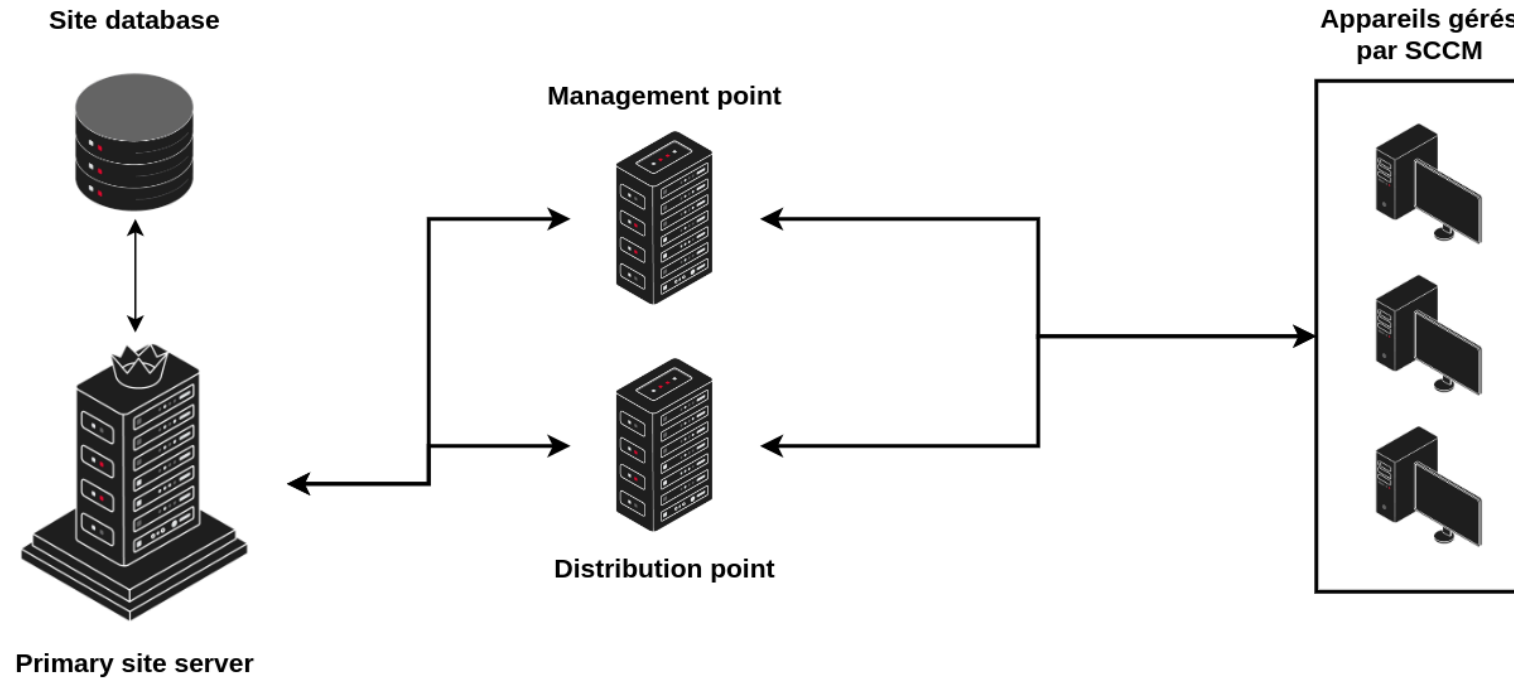
Introduction

- SCCM (MECM) est une solution de management d'appareils au sein d'environnements Active Directory
- Un agent est installé sur les appareils gérés par SCCM
- **Les politiques sont un élément fondamental de SCCM**
- Elles représentent les configurations appliquées aux appareils (mises à jour, déploiement d'applications, scripts etc.)



Les politiques SCCM : contexte et concepts

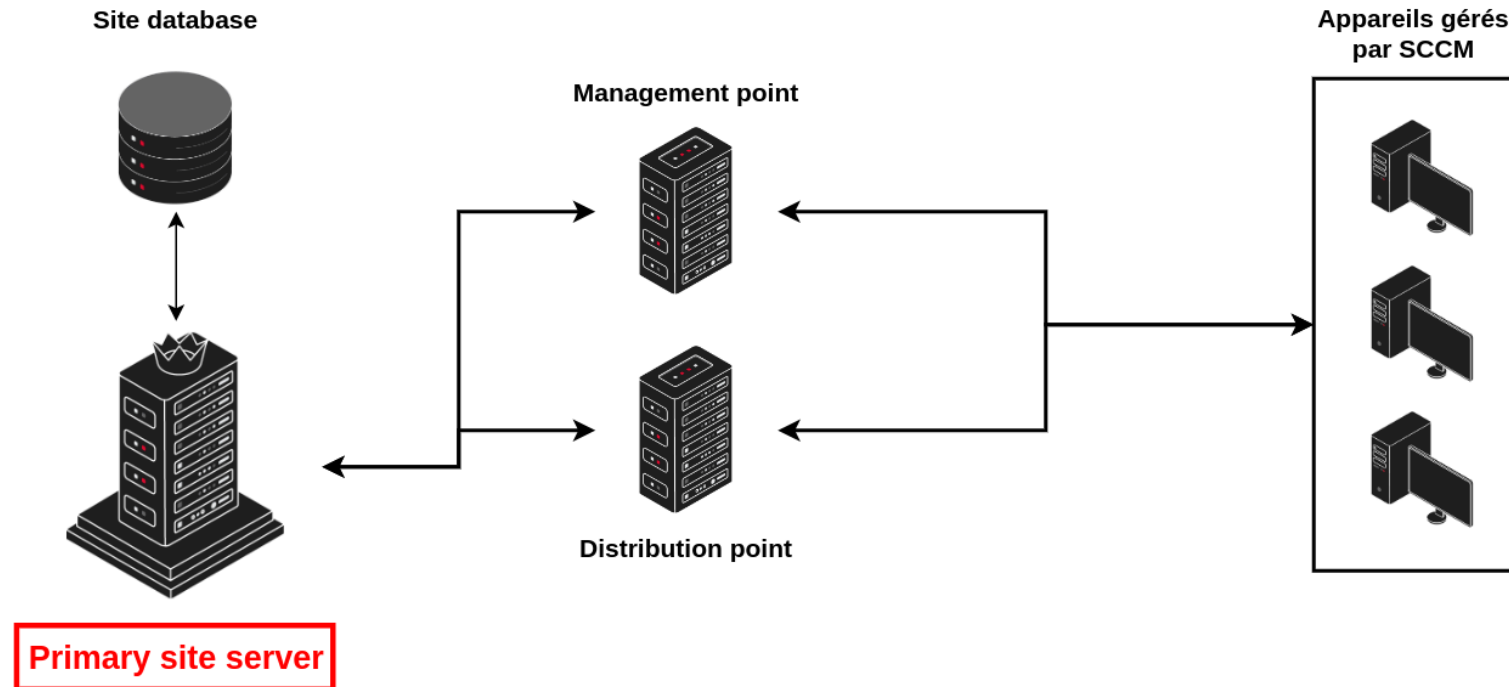
Topologie SCCM



Topologie simplifiée de SCCM

Les politiques SCCM : contexte et concepts

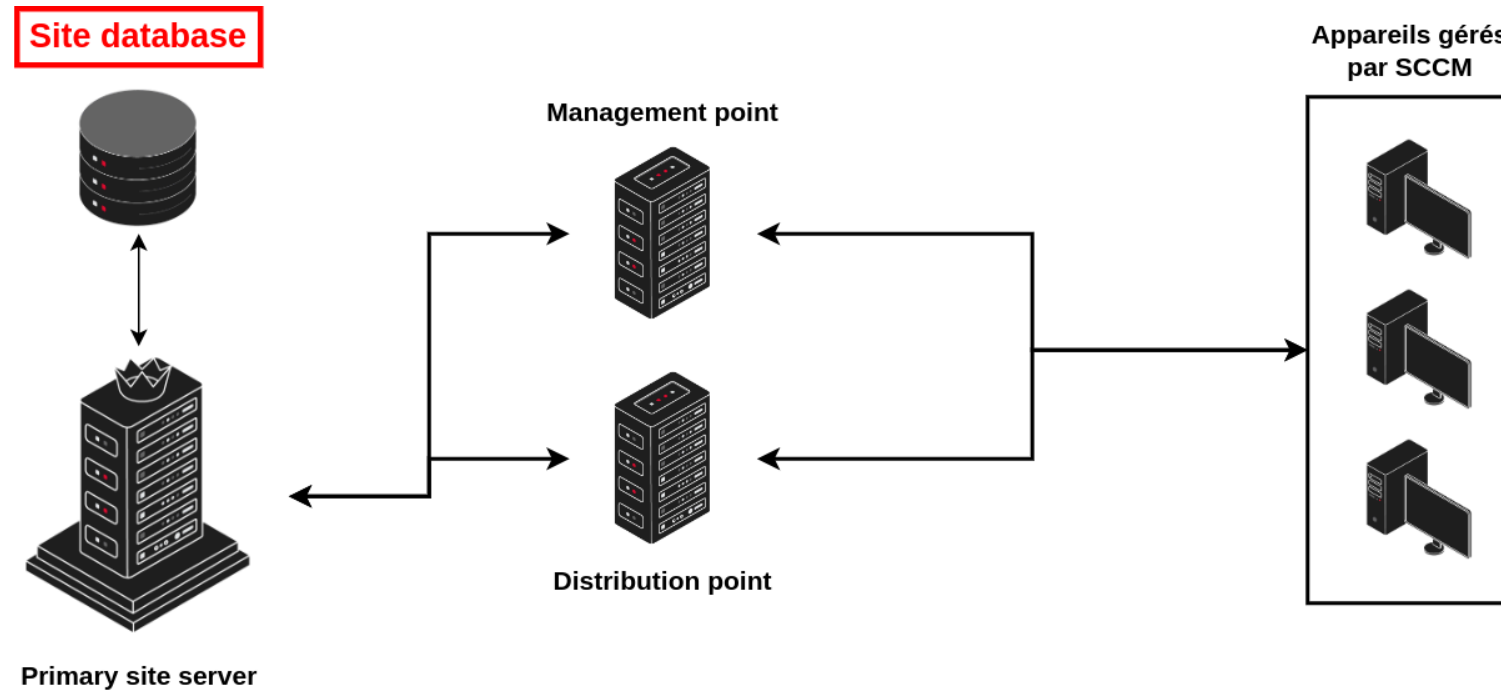
Topologie SCCM



Primary site server : Serveur sur lequel le site SCCM a été installé. Implémente par défaut les différents composants SCCM et fournit une interface de management aux administrateurs.

Les politiques SCCM : contexte et concepts

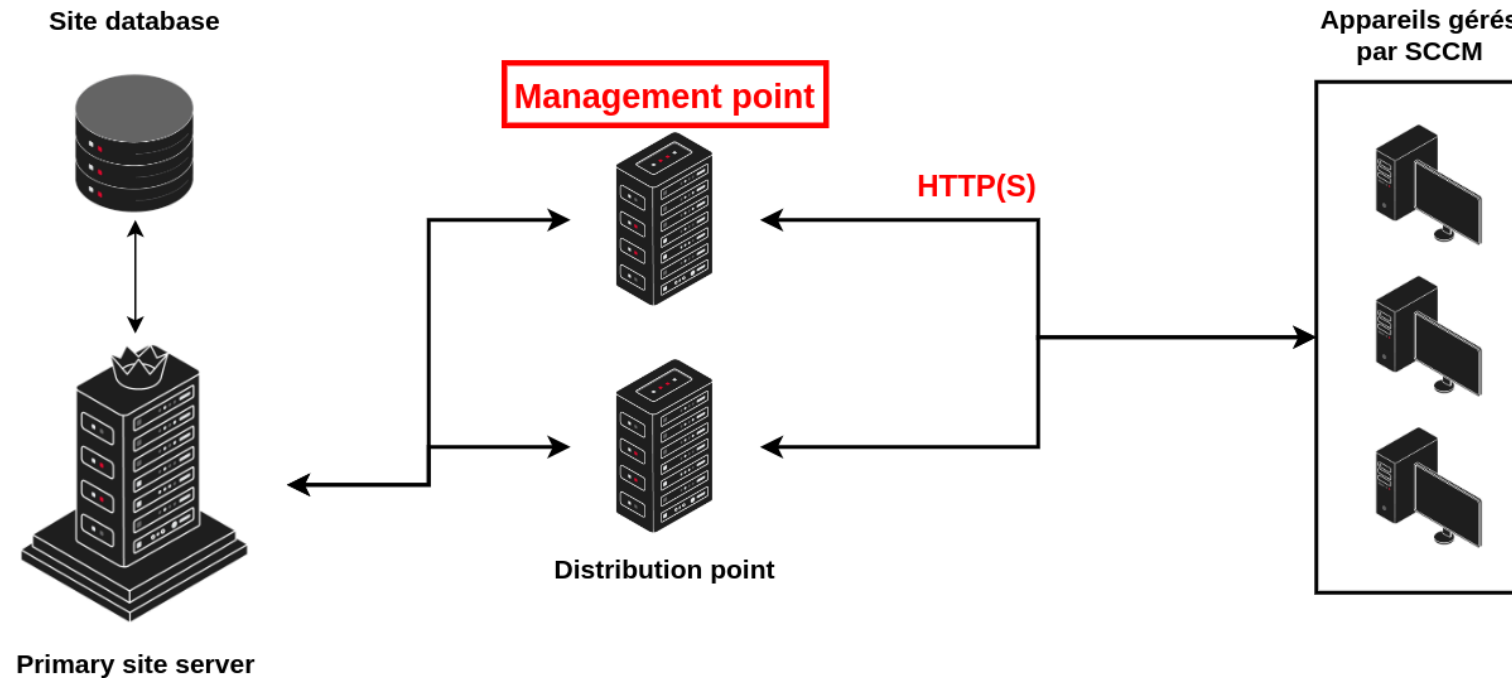
Topologie SCCM



Site database : La base de données hébergeant les données utilisées par l'infrastructure SCCM.

Les politiques SCCM : contexte et concepts

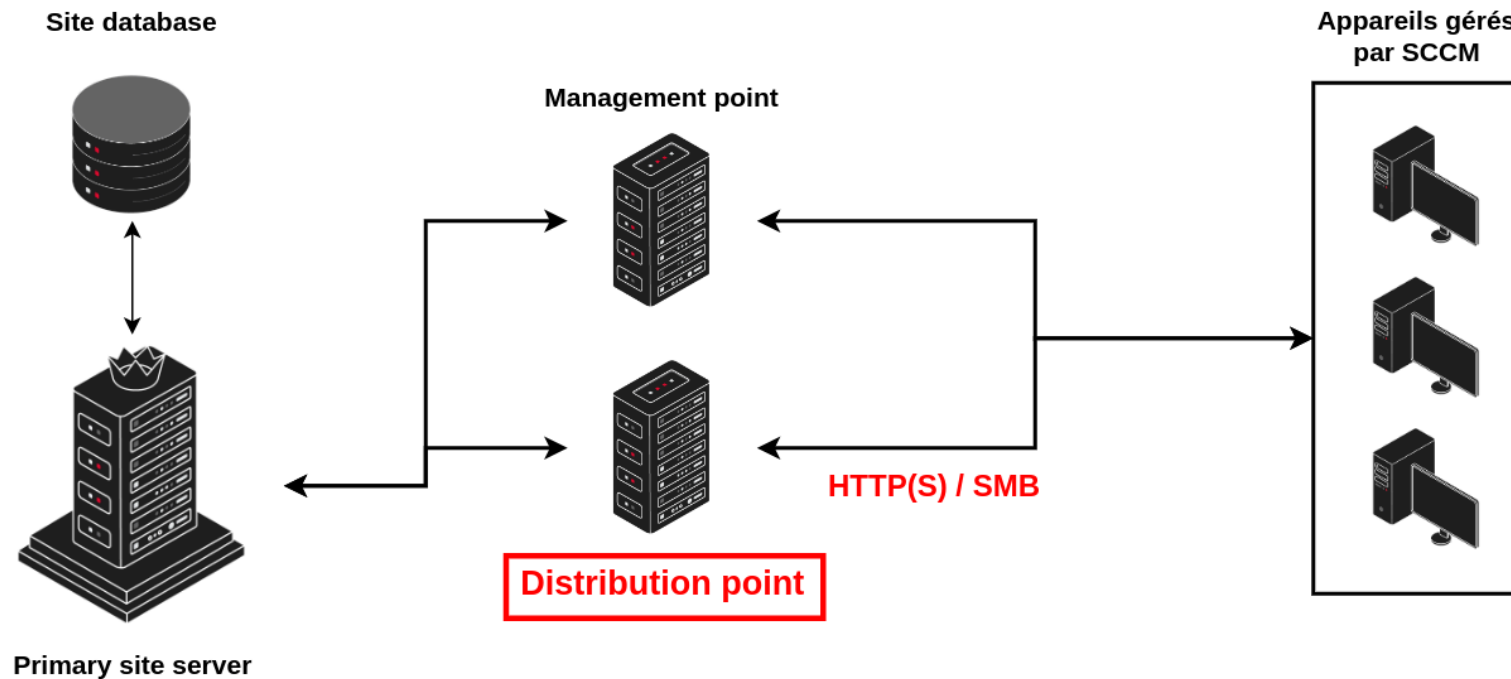
Topologie SCCM



Management Point : Le Management Point (MP) est l'intermédiaire entre les appareils gérés et SCCM. **Il communique les politiques SCCM aux clients.** Ces politiques sont transmises via HTTP/HTTPS sous la forme de documents XML interprétés par le client SCCM, qui applique ensuite les configurations désirées.

Les politiques SCCM : contexte et concepts

Topologie SCCM



Distribution Point : Un Distribution Point (DP) héberge le **contenu volumineux utilisé par les politiques** (fichiers d'installation, applications, images de systèmes d'exploitation, etc.). Le contenu est rendu disponible via HTTP(S) ou SMB.

Les secrets au sein des politiques SCCM

Les secrets au sein des politiques SCCM

Secrets intégrés au contenu des politiques

- Certaines politiques SCCM contiennent des identifiants
- **Network Access Account (NAA)**
 - Probablement la politique SCCM la plus connue d'un point de vue offensif
 - Politique transmise à tous les appareils SCCM
 - Contient les identifiants d'un compte du domaine
 - Supposé être un compte non-privilégié (ce qui n'est régulièrement pas le cas)
- **Task sequences**
 - Série d'actions exécutées automatiquement sur les clients
 - Certaines étapes sont configurées avec des identifiants (runas, connexion à un share etc.)
- **Collection variables**

Les secrets au sein des politiques SCCM

Les fichiers des Distribution Points

- Comme évoqué précédemment, les Distribution Points hébergent les ressources utilisées par les politiques SCCM
- Ces fichiers peuvent être inoffensifs (fichiers d'installation, clés publiques etc.)
- Mais on peut y trouver des fichiers sensibles (scripts Powershell, clés privées, fichiers de configuration etc.)
- Par défaut, **une authentification du domaine est nécessaire pour télécharger les ressources du DP** (HTTP/SMB)

Exploiter la distribution des politiques SCCM : attaques et défauts de configuration

Attaques et défauts de configuration

Extraction des ressources des Distribution Points

- La méthode la plus directe d'extraction de secrets consiste à télécharger les ressources hébergées sur les Distribution Points
- Cette action ne nécessite qu'une authentification du domaine

❗ DP01: S'authentifier auprès des Distribution Points et rechercher des ressources sensibles de politiques SCCM pour élever ses privilèges

- Peut être exploité via HTTP/HTTPS (**SCCMSecrets**) ou SMB (**CMLoot**)

Attaques et défauts de configuration

Extraction des ressources des Distribution Points

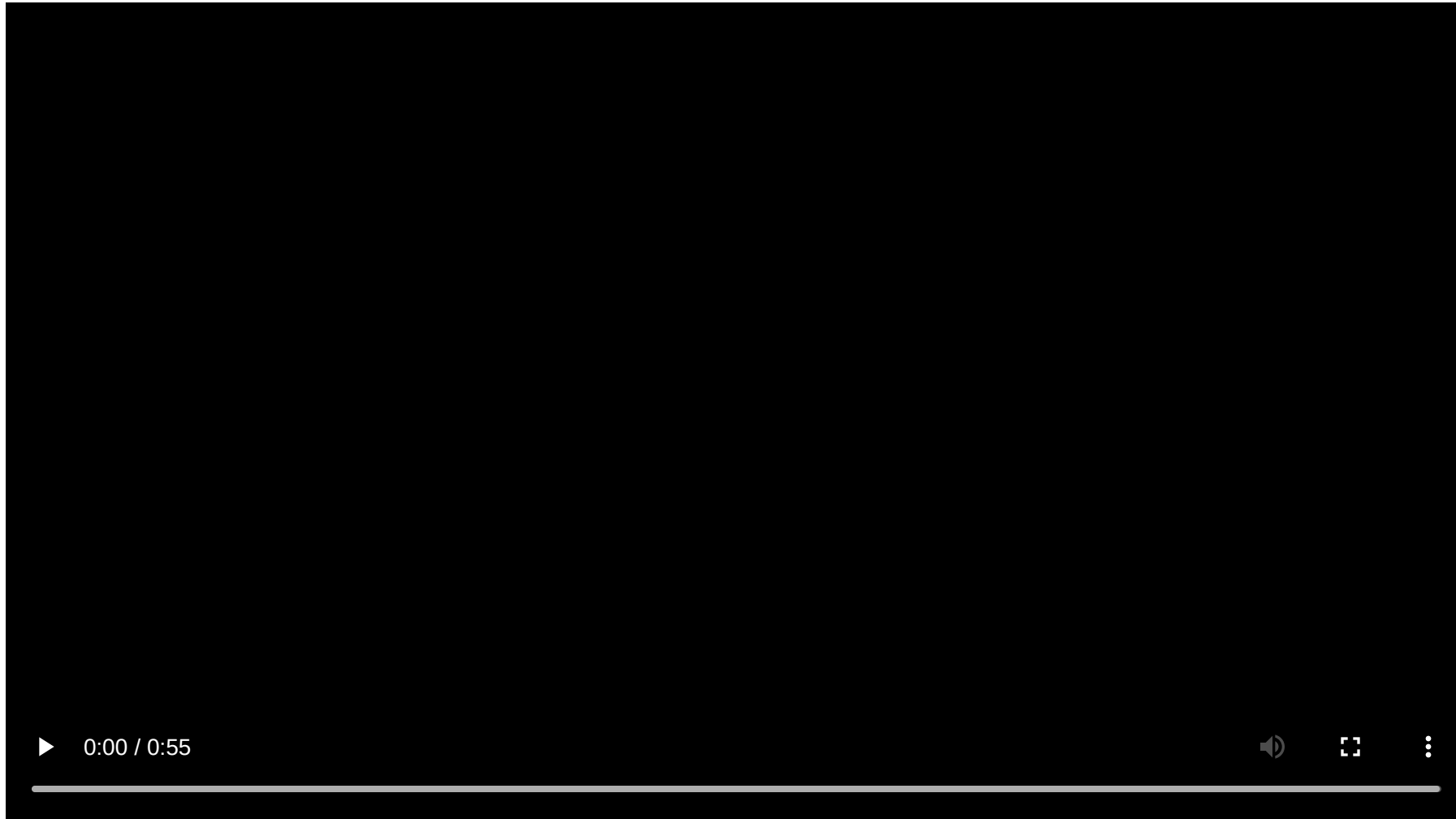
- Les Distribution Points peuvent être configurés pour permettre **l'accès anonyme**
- Pas d'authentification nécessaire pour accéder aux ressources **via HTTP(S)**
- Peut être exploité par un attaquant sans identifiants pour accès initial

⚠ DP02: Exploiter l'accès anonyme aux Distribution Points via HTTP(S) pour rechercher des ressources sensibles sans aucune authentification.

- Peut être exploité via **SCCMSecrets** ou **sccm-http-looter**

Attaques et défauts de configuration

Démonstration



Attaques et défauts de configuration

Récupération des politiques secrètes depuis le Management Point

- Le contenu des politiques elles-mêmes est également intéressant
- Les politiques sont distribuées par les MPs aux **clients SCCM enregistrés**
- Pour s'enregistrer, un appareil génère un **certificat auto-signé**
- Les communications avec le Management Point sont alors signées avec la clé privée
- La soumission initiale du certificat pour enregistrement peut être effectuée de **deux manières**

Attaques et défauts de configuration

Récupération des politiques secrètes depuis le Management Point



- > L'appareil est enregistré, mais **non approuvé**
- > Approbation manuelle par un administrateur requise
- > **Impossibilité d'accéder aux politiques secrètes**

- > L'appareil est enregistré **et approuvé**
- > **Possibilité d'accéder aux politiques secrètes**

Attaques et défauts de configuration

Récupération des politiques secrètes depuis le Management Point

- ❗ MP01: Utiliser un compte machine du domaine pour enregistrer un appareil SCCM approuvé et récupérer les politiques secrètes depuis un Management Point
 - Peut être exploité avec **SCCMSecrets**

Attaques et défauts de configuration

Récupération des politiques secrètes depuis le Management Point

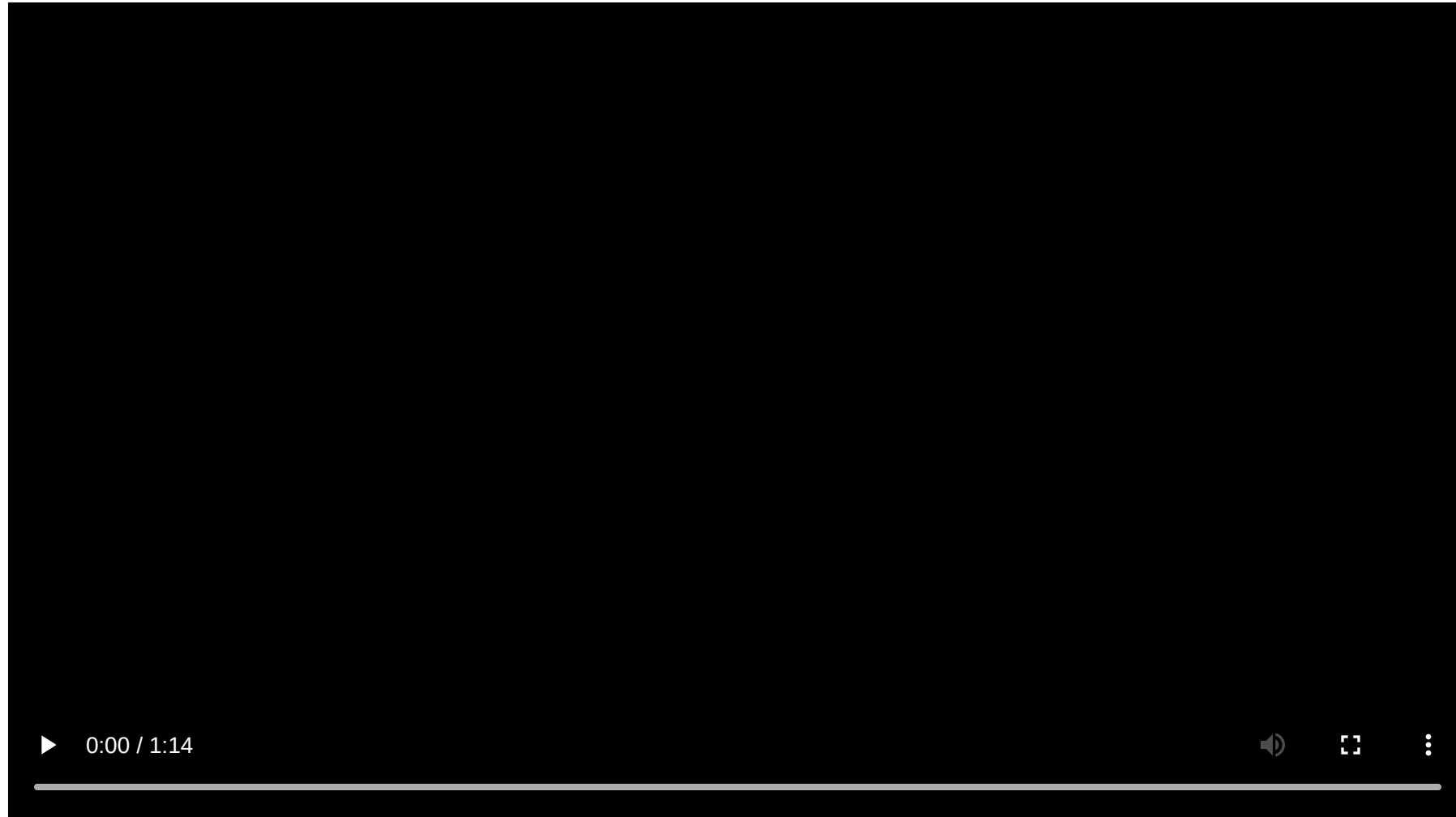
- SCCM peut être configuré pour **approuver automatiquement les appareils s'enregistrant via la méthode anonyme**
- Un attaquant non-authentifié peut enregistrer un appareil et récupérer les politiques secrètes

⚠ MP02: Exploiter l'approbation automatique des appareils pour enregistrer anonymement un nouvel appareil dans SCCM, et récupérer les politiques secrètes associées aux collections par défaut

- Peut être exploité avec **SCCMSecrets**

Attaques et défauts de configuration

Démonstration

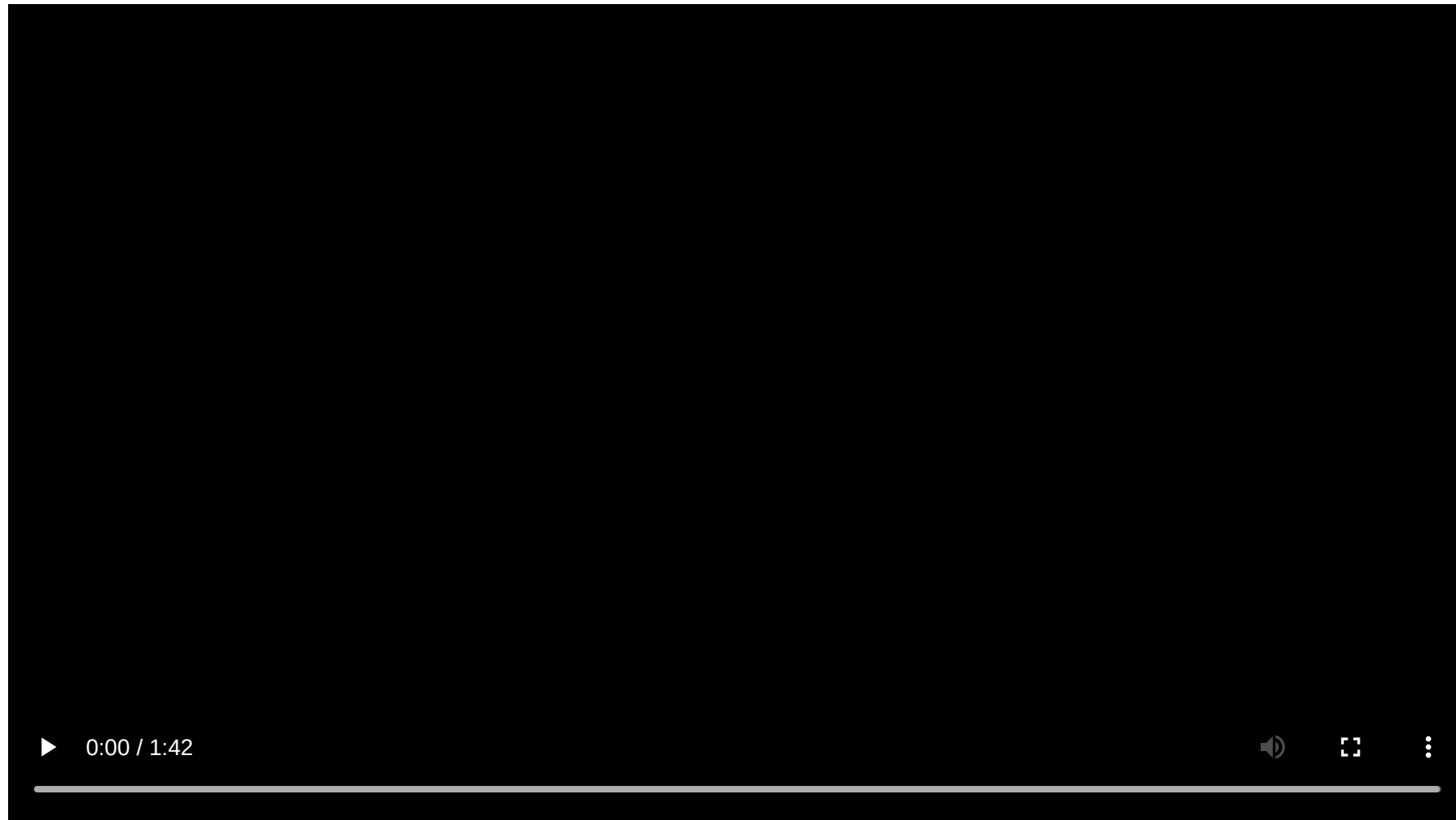


Attaquer les politiques SCCM par relai

Attaquer les politiques SCCM par relai

- Authentification du domaine pour :
 - Accéder aux ressources des Distribution Points
 - Enregistrer des appareils sur les Management Points
- L'authentification du domaine via HTTP est une **cible idéale pour le relai**
- Les attaques décrites précédemment peuvent être effectuées via relai NTLM (et Kerberos)
- Pas d'identifiants nécessaires – seulement une position de Man-in-the-Middle
- Nous avons implémenté ces attaques dans **ntlmrelayx.py** fin 2024

Attaquer les politiques SCCM par relai



Considérations défensives

- De manière générale, **forcer l'utilisation de HTTPS rend les différentes attaques présentées plus difficiles à implémenter** en raison de l'authentification cliente mTLS
- Passer en revue les secrets distribués via les politiques SCCM
- **Distribution Points** : ne pas permettre l'accès anonyme
- **Management Points** : ne pas activer l'approbation automatique des appareils
- **Attaques par relai** : forcer l'utilisation d'HTTPS et activer l'Extended Protection for Authentication (EPA) sur les répertoires virtuels `SMS_MP_WindowsAuth` et `SMS_DP_SMSPKG$` (rester progressif sur l'activation EPA en fonction des impacts fonctionnels)

Merci !

- <https://github.com/synacktiv/SCCMSecrets>

SYNACKTIV



<https://www.linkedin.com/company/synacktiv>



<https://x.com/synacktiv>



<https://synacktiv.com>



<https://bsky.app/profile/synacktiv.com>