Understand Umbrella Encryption for AD Sync

Contents

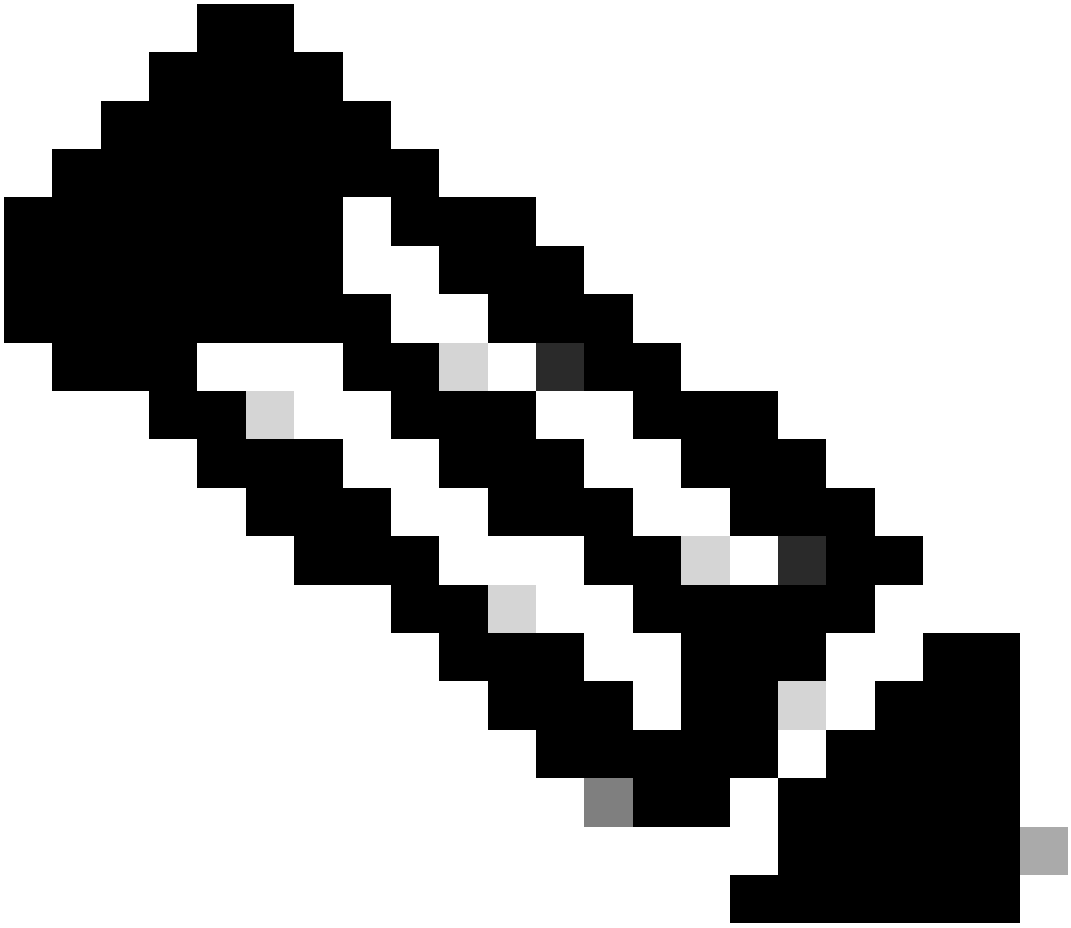
Introduction

This document describes Umbrella encryption for AD sync, such as how this data trasfer is encrypted.

Background Information

The Umbrella AD Connector software retrieves details of User, Computer, and Group information from your AD Domain Controller using LDAP. Only the necessary attributes are stored from each object, this includes ***sAMAccountName***, ***dn***, ***userPrincipalName, memberOf***, ***objectGUID, primaryGroupId*** *(for users and computers)*, and ***primaryGroupToken*** *(for groups)*.

This data is then uploaded to Umbrella for use in Policy Configuration and Reporting. This data is also required for per-user or per-computer filtering.



Note: objectGUID is sent in hashed form.

To find out exactly what is being synced, you can look at the .ldif files contained within:

```
C:\Program Files\OpenDNS\OpenDNS Connector\ADSync\*.ldif
```

This article describes how this data transfer is encrypted.

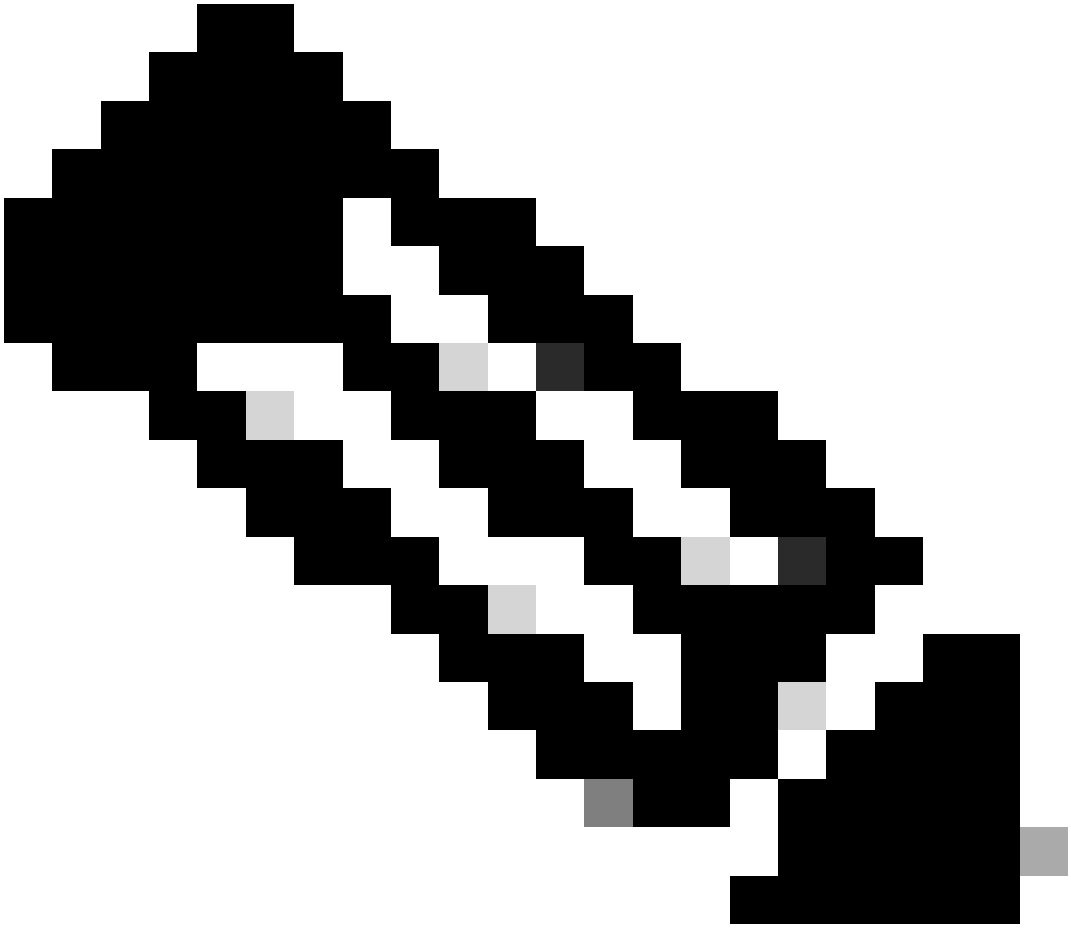
Encryption for AD Data Upload

The Umbrella AD Connector uploads the AD information to Umbrella using a secure HTTPS connection. The upload between the *Connector* <> *Umbrella* cloud is always encrypted.

Encryption for AD Data Retrieval

As of v1.1.22 the Connector now attempts to retrieve user details with encryption between *Domain Controller <> Connector*. Two methods are attempted:

- **LDAPS**. Data is transmitted over a secure tunnel.
- **LDAP with Kerberos authentication**. Provides packet-level encryption.



> **Note**: LDAPS is not used when the Connector software is running on the same server as the Domain Controller used for ADsync.

If this attempt fails for any reason it reverts to this mechanism:

- **LDAP with NTLM authentication**. This provides secure authentication but the data transfer between the *DC > Connector* happens without encryption.

To ensure that encryption is possible we recommend to:

- **Enable LDAPS on your Domain Controller(s)**. This is beyond the scope of Umbrella support, but can be enabled with Microsoft's documentation.
- **Ensure that the hostname of your Domain Controller(s) is correctly configured** in *'Deployments > Sites and AD'*. The correct hostname is required for both encryption methods. If the hostname is

incorrect for any reason we recommend to re-register the Domain Controller using our configuration script, or contact Umbrella support.

To confirm encryption is happening. You can check the log file here:

```
C:\Program Files (x86)\OpenDNS\OpenDNS Connector\<VERSION>\OpenDNSAuditClient.log
```

During AD sync, you see log entries such as:

LDAPS connection successful:
Using SSL for <SERVER> communication to fetch the DN.

Kerberos authentication successful:
Using Kerberos for <SERVER> communication to fetch the DN.

NTLM failback mechanism in use:
Kerberos failed for DC Host <SERVER>. The hostname can be invalid. Falling back to NTLM query.