CHAPTER 1

# Getting Started with Connector

**Revised: July 18, 2011**

## Overview

This chapter will help you decided when to deploy Connector and the most appropriate deployment method for your network infrastructure. Connector is used to deliver web traffic from a client computer to Cisco Cloud Web Security. You may not need to use Connector. It is required in the following configurations only:

- When user-level granularity is required for policy and reporting.
- When accessing the Cloud Web Security from a device with a dynamic IP address.
- When accessing Cloud Web Security off-site or with a roaming device without Cisco AnyConnect Secure Mobile Security installed.

## Basic Operations

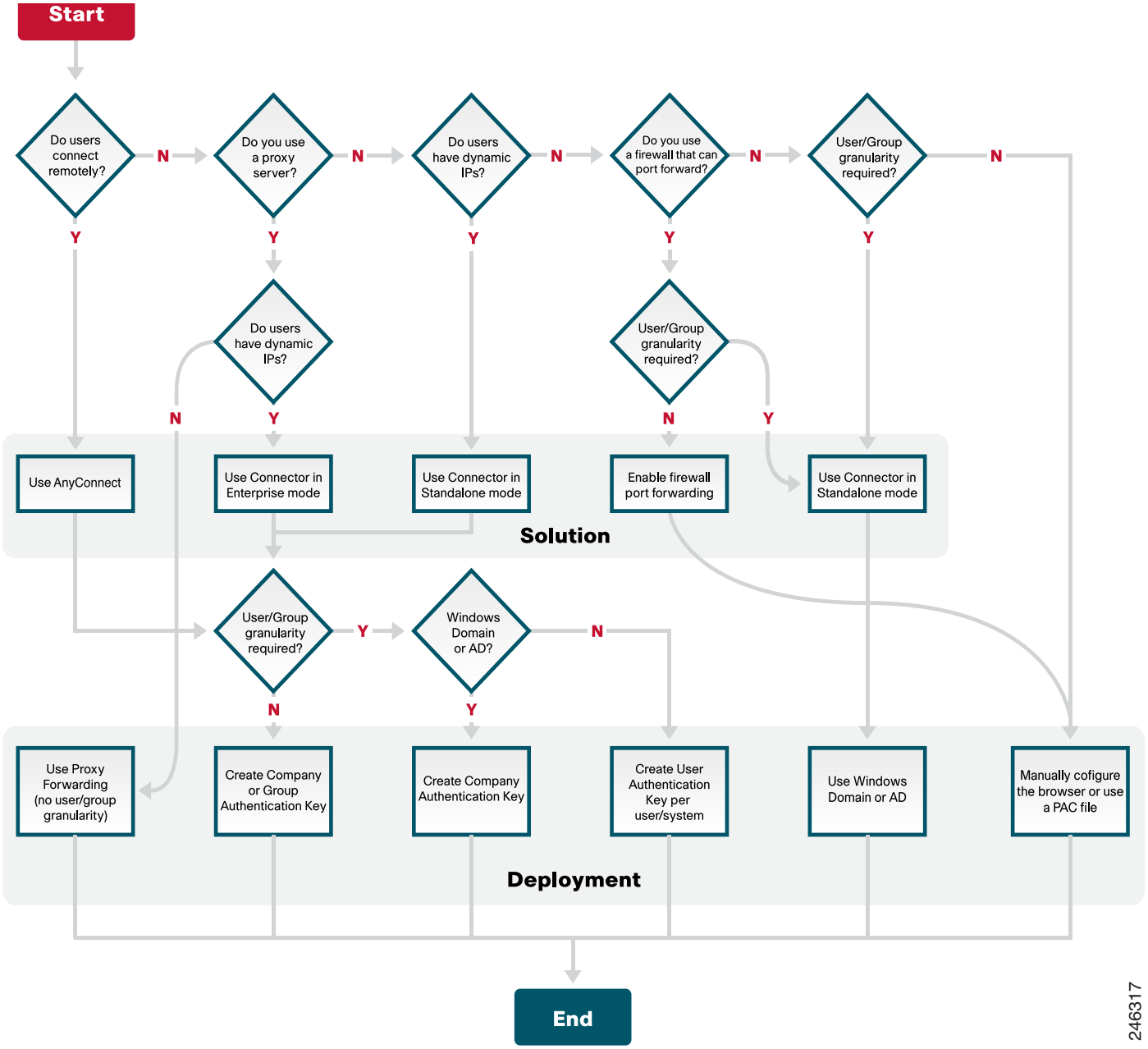
Connector identifies users by merging their details from Active Directory using LDAP, or Windows Domain integration and an authentication key. With Connector, users with a dynamic IP address can connect to Cloud Web Security with a company, group, or user authentication key. Users with a static IP address do not require a key.

Connector encrypts user information which Cloud Web Security uses to apply specific user or group policy information. Connector passes user web traffic requests through Cloud Web Security for filtering, scanning, and policy enforcement, before providing the cleansed web content to the user.

Company, Group, and User authentication keys are created in ScanCenter. For further information see the ScanCenter Administrator Guide. These enable Cloud Web Security to identify and authenticate a user. Group authentication keys provide more detailed user behavior reporting and policy management, but may require additional key management by the administrator.

# Choosing a Connector Mode and Authentication Key Type

Before installing Connector, use the following flow chart to decide the Connector mode (standalone or enterprise) and Authentication Key (Company, Group, or User) are most appropriate for your organization.



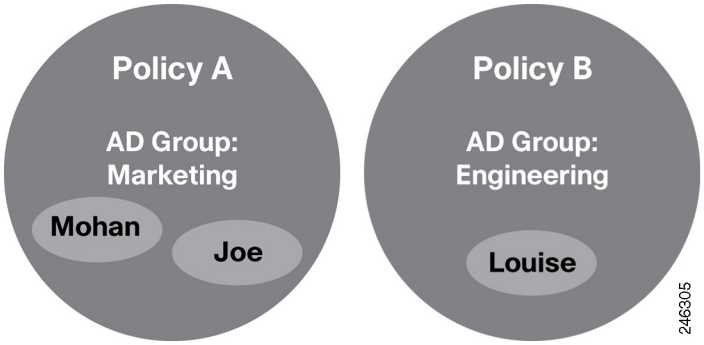
# Deployment Scenarios

When you have chosen your appropriate solution and deployment method, based on your network infrastructure, you are ready to proceed. The flow chart provides for a variety of deployment scenarios, but in practise the three most common are:

- Company authentication key and Active Directory
- Group authentication key
- User authentication Key

## Company Authentication Key and Active Directory

The most common scenario uses a single company authentication key for all users in the organization and Active Directory to provide User and Group granularity for policy and reporting. An example is shown below.




To create this configuration:

**Step 1** Create two Active Directory groups in ScanCenter:

- WinNT://…/Marketing
- WinNT://…/Engineering

**Step 2** Install Connector and the company authentication key on the Domain Controller.

**Step 3** Apply Policy A to the Marketing group and Policy B to the Engineering group.

In this scenario, Policy A is applied to Mohan and Joe, while Policy B is applied to Louise.

If a policy causes a block event for Mohan or Joe, it will be registered against WinNT://.../Marketing with User information for Mohan or Joe. Block events for Louise, it will be registered against WinNT://.../Engineering with her user information.

## Group Authentication Key

The next most common scenario uses a group authentication key without Active Directory. In the following example, Connector is installed in standalone mode with a location-based key (LK), a unique group authentication key, in each of three branch offices.


To create this configuration:

**Step 1** Create a group authentication key for each location group (NYGROUP, LDNGROUP, TKYGROUP).

**Step 2** Install Connector in standalone mode and the relevant group authentication key at each location.

**Step 3** Apply Policy A to group NYGROUP, Policy B to LDNGROUP, and Policy C to TKYGROUP.

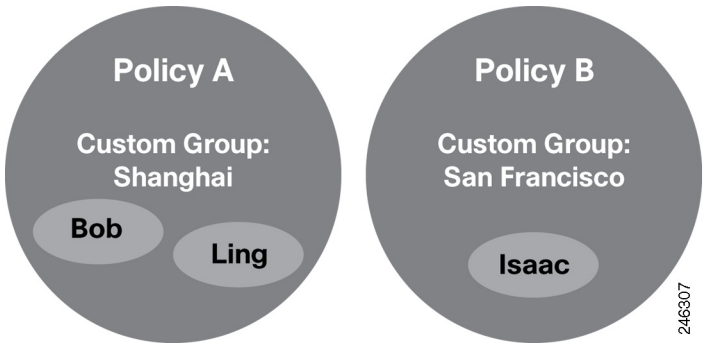
In this scenario, Policy A is applied to Sinead and Joe, Policy B is applied to Adeola, and Policy C is applied to Yuki.

If a policy causes a block event for Sinead or Joe, it will be registered against NYGROUP group. Block events for Adeola, it will be registered against the LDNGROUP group. Block events for Yuki will be registered against TKYGROUP.

**Note** This deployment method is suitable only when Active Directory is not used.

# User Authentication Key

This scenario provides an alternative off-site solution when it is not possible to deploy Cisco AnyConnect Secure Mobile Security or Passive Identity Management. For example, it could be used for non-Windows users. In the following example, Connector and a user authentication key are installed on each user's computer.




To create this configuration:

**Step 1** Create a custom groups and assign users to those groups in ScanCenter.

**Step 2** Create a user authentication key for each user in ScanCenter.

**Step 3** Install Connector in standalone mode and a unique user authentication key on each computer.

In this scenario, Policy A is applied to Bob and Ling and Policy B is applied to Isaac. If a policy causes a block event for Bob, Ling, or Isaac it will be registered against their User and Custom Group.

**Caution** The user authentication key overrides all reported user information. Therefore you must deploy the key only once with a separate Connector installation for each computer.

## Summary

When Active Directory is in use, a company key installed with Connector in standalone or enterprise mode on the Domain Controller will provide user and group granularity for policy and reporting.

If you have satellite offices where you want to apply group policy you should use a group authentication key.

For portable computers or remote connections where Cisco AnyConnect Secure Mobile Security or Passive Identity Management are not viable, a user authentication key and a local installation of Connector in standalone mode should be used.

# Authentication Process

Connector uses one of several possible authentication resources to annotate web requests with end-user data. The supported data sources are:

- Active Directory (using the LDAP protocol)
- Windows Domain (for example via CIFS / SMB protocols)
- Authentication Key

When a Company Authentication Key is used in conjunction with either Active Directory or Windows Domain lookup, data needs to be ‘merged.’ See Company Authentication Key and Active Directory, page 1-3.

There are several ways to use the authentication key:

- As end-user identification (with Cisco AnyConnect Secure Mobile Security where appropriate)
  - To control access to Cloud Web Security
  - To identify an organization
  - To identify groups (within an organization)
  - To identify users (within groups)
- As group identification (with Cisco AnyConnect Secure Mobile Security where appropriate)
  - To control access to Cloud Web Security
  - To identify an organization

  - To identify groups
- As organization identification (in enterprise mode for dynamic IP access)
  - To control access to Cloud Web Security
  - To identify an organization

As you can see, the authentication key has a dual purpose:

- To control access to Cloud Web Security (as opposed to using static IP lockdown)
- To provide some identification data

Data embedded in requests can be classified as follows:

- Service authentication data (optional if you use static IP addresses)
  - Authentication key
- User identification data
  - Internal IP address
  - User name
  - Groups (for example from AD or Windows Domain)
- Session data
  - Local time
  - Tallies

**Note** Data is combined and transmitted securely with every web request via data headers.

# Groups and Policy Application

The following sections describe how user data is derived, how groups work, and how policies are applied in ScanCenter.

## Deriving User Data

ScanCenter derives user data from the maximum granularity available for a given request; the user name will be chosen from the first available data item:

- Connector-supplied user name (either from Active Directory or from user Authentication Key. If both, Connector uses User Authentication Key user name)
- Basic digest auth user name (for customers who have Squid)
- Connector-supplied internal IP
- Squid internal IP (for customers who have Squid)
- External IP

# Applying Policy to Groups

Within ScanCenter there are two basic group types:

- Active Directory groups: must be created to match those returned by the Connector (from a customer's Active Directory server).
- Custom groups: collections of other identification (for example user names, internal IPs, external IPs)

A group authentication key can be assigned to either an Active Directory group or to a Custom Group.