# Silverback Best Practices

# Windows (Phone) Alternative Enterpriseenrollment SSL Approach

**For internal use & confidential**

© Matrix42 AG
This document is only for internal use and marked as confidential

## Table of Content

Windows (Phone) Enrollment Basics
Silverback Cloud Deployments using the Cloud Connector

© Matrix42 AG
This document is only for internal use and marked as confidential

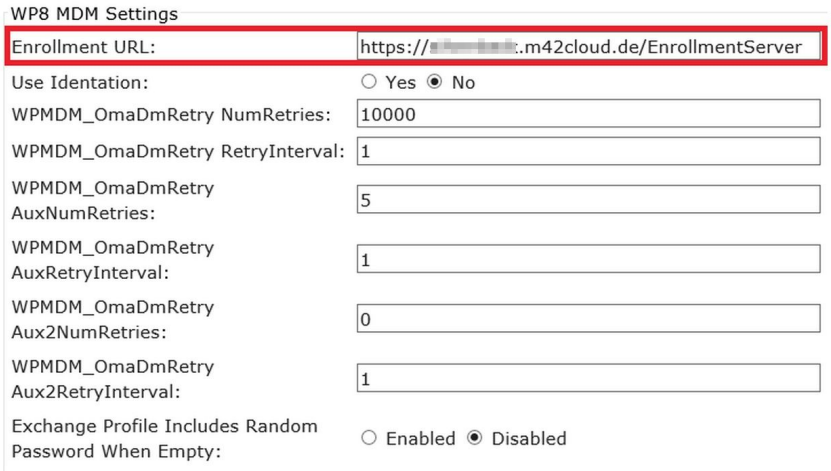
## Windows (Phone) Enrollment Basics

### How Windows (Phone) will find Silverback

A Windows (Phone) device will try and find the Silverback Server by using an AutoDiscover technology that is similar to Exchange ActiveSync. The Device will take the Username that is entered in to the Workplace App and isolate the Domain Suffix entered.If a user enrolls with user01@imgagoverum.com, the device will try and find https://enterpriseenrollment.imagoverum.com .

### How Silverback Tells the Device it's Management URL

Assuming that the device can find the enterpriseenrollment.imagoverum.com it will talk to the 'EnrollmentServer' site within Silverback Website, which will give read the URL as configured in the Silverback Settings Page.




The device will save this URL, and then continue communicating with the Silverback Server as part of its enrollment.

© Matrix42 AG
This document is only for internal use and marked as confidential

## Silverback Cloud Deployments using the Cloud Connector

### The Problem

In Cloud Based Deployments the Silverback Server is typically hosted using a *.m42cloud.net or *.silverbackmdm.com SSL Certificate, but the users will be enrolling with their email address which will be different.

Working Example:
Silverback Server: https://silverback.m42cloud.net
User Enrolling: user01@imagoverum.com

As described in the previous section, we know that the Windows Phone Device will try and find https://enterpriseenrollment.imagoverum.com - but this is not the URL of our Silverback Server, so the Autodiscover will fail.

### The Solution

Using DNS we are able to 'mask' this problem so Autodiscover continues to work and the device will enroll. As the customer enrolling will own their email domains, we simply ask them to put the 'enterpriseenrollment' DNS Entry in their Domain, but point this to our Cloud Based Instance. This can be done with either an 'A' record, or a 'CNAME' record depending on the nature of your Silverback Environment.

The MDM Engine inside the Windows (Phone) device is smart enough to see the redirect and warn the user of this event. When the user press 'Continue' the device enrollment process continuous as designed, and the device gets registered in Silverback.

© Matrix42 AG
This document is only for internal use and marked as confidential