



**Deepnet Unified Authentication  
for Citrix Web Interface  
User Guide**

**Copyright 2007,  
Deepnet Security Limited.**

**Trademarks**

Deepnet Unified Authentication, MobileID, QuickID, PocketID, FlashID, SmartID, TypeSense, VoiceSense, MobilePass, DevicePass, RemotePass and Site Stamp are trademarks of Deepnet Security Limited. All other brand names and product names are trademarks or registered trademarks of their respective owners.

**Copyrights**

Under the international copyright law, neither the Deepnet Security software or documentation may be copied, reproduced, translated or reduced to any electronic medium or machine readable form, in whole or in part, without the prior written consent of Deepnet Security.

**Licence Conditions**

Please read your licence agreement with Deepnet carefully and make sure you understand the exact terms of usage. In particular, for which projects, on which platforms and at which sites, you are allowed to use the product. You are not allowed to make any modifications to the product. If you feel the need for any modifications, please contact Deepnet Security.

**Disclaimer**

This document is provided "as is" without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the document. Deepnet Security may make improvements of and/or changes to the product described in this document at any time.

**Contact**

If you wish to obtain further information on this product or any other Deepnet Security products, you are always welcome to contact us.

Deepnet Security Limited  
The Maples Business Centre  
144 Liverpool Road  
London, N1 1LA  
United Kingdom

Tel: +44(0)20 7700 4282  
Fax: +44(0)20 7697 8282  
[www.deepnetsecurity.com](http://www.deepnetsecurity.com)  
[support@deepnetsecurity.com](mailto:support@deepnetsecurity.com)

---

# Table of Contents

Overview .....3

Installation .....4

    Installation Prerequisites.....4

    Installation Procedure.....4

    Configure Authentication Platform.....6

    Configure CWI Agent.....6

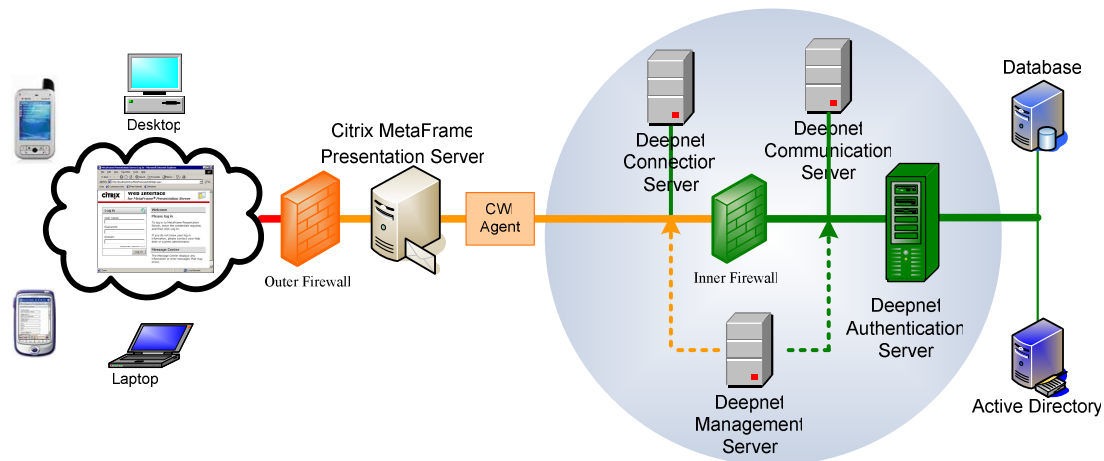
Authentication .....9

## Overview

Citrix Web Interface (CWI) is an application deployment system that provides users with access to Citrix MetaFrame applications through a standard Web browser. Each user is presented with all the applications published in the MetaFrame server farms for that user. With the Web Interface, administrators have centralized application management capabilities and complete control over the application deployment process.

Deepnet Unified Authentication for CWI enables strong two-factor authentication for the Citrix Web Interface Logon form, requiring a user to authenticate with a second factor credential such as one-time password before access to the site is allowed.

Deepnet Unified Authentication for CWI is one of many enterprise solutions that the Deepnet Unified Authentication Platform supports. The following diagram illustrates the typical components involved in the Deepnet Unified Authentication for CWI solution:



The complete solution consists of the following components:

- Deepnet Unified Authentication Platform
- Deepnet Citrix Web Interface (CWI) Agent

The Deepnet Citrix Web Interface (CWI) Agent acts as the bridge that connects the Citrix MetaFrame Presentation Server and the Deepnet Authentication Server.

The CWI agent is installed on each computer running Citrix Presentation Server to replace the standard Citrix Web Interface login form with Deepnet's two-factor authentication login form.

## Installation

### Installation Prerequisites

- Deepnet Unified Authentication Platform installed and registered. Please refer to the User Guide of the Platform for details.
- Citrix MetaFrame Presentation Server 4.0.

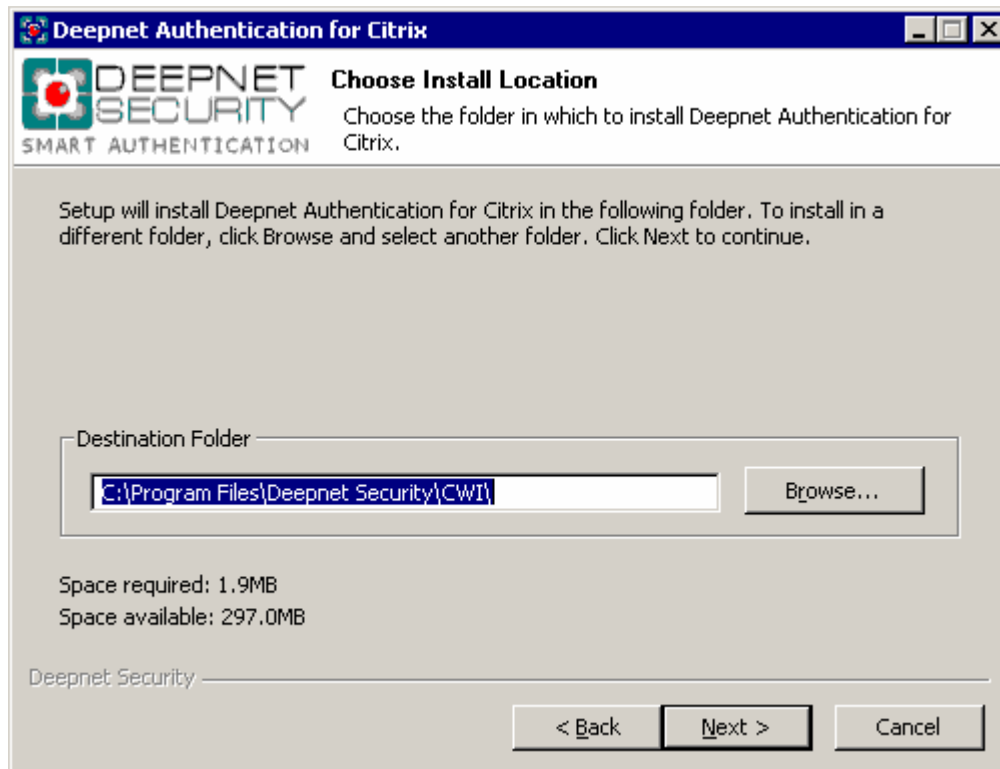
### Installation Procedure

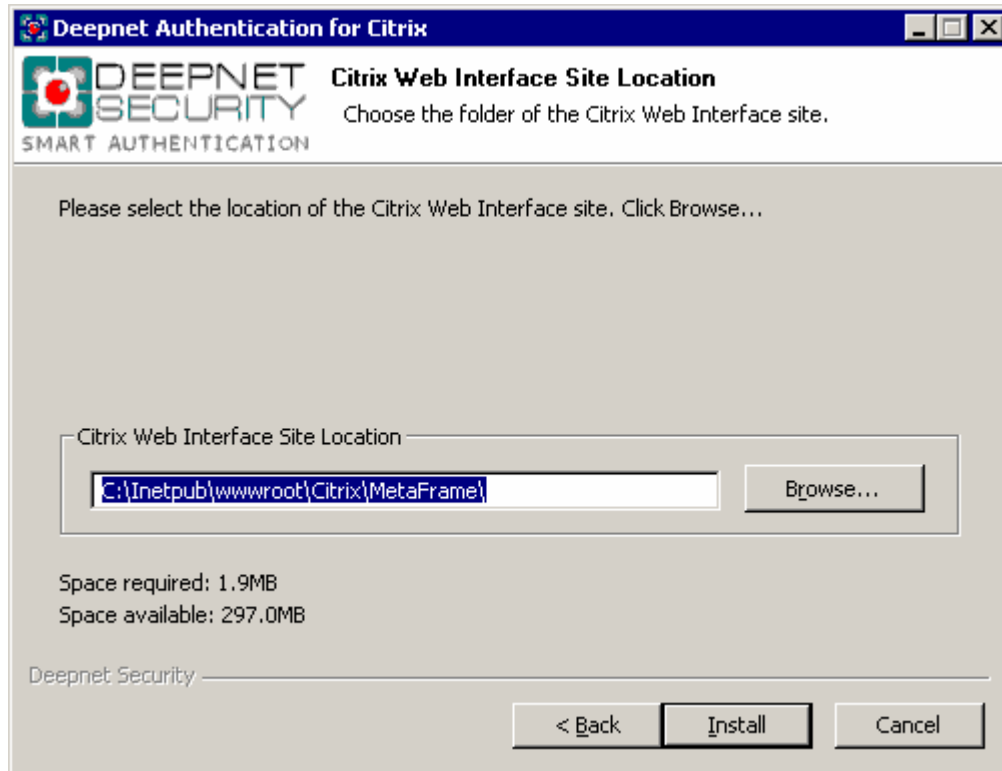
Deepnet Unified Authentication for CWI should only be installed after the Deepnet Unified Authentication Platform has been successfully installed and operational.

Deepnet Unified Authentication for CWI should be installed on the machine on which the Citrix MetaFrame Presentation Server is installed and operating.

To install the Deepnet Unified Authentication for CWI, simply launch the installer "SetupCWI.exe" and go through the following steps:

- Step 1: Introduction**
- Step 2: Licence Agreement**
- Step 3: Choose Install Folder**
- Step 4: Choose Citrix Web Site Location**
- Step 5: Install Complete**





At this step, you need to choose the location of the Citrix web site where you want to add two-factor authentication features provided by Deepnet authentication.

## Configuration

After the successful installation of Deepnet Unified Authentication for CWI (the Authentication Agent), you need to configure the following components:

- Deepnet Authentication Platform
- Deepnet CWI Agent

### Configure Authentication Platform

Deepnet Unified Authentication Platform can support multiple applications. Depending on your company's IT infrastructure and security policy, you may set up different applications for different types of access. For instance, one application for VPN remote access, one for Windows logon and one for CWI. You can, of course, set up just one application for all types of access.

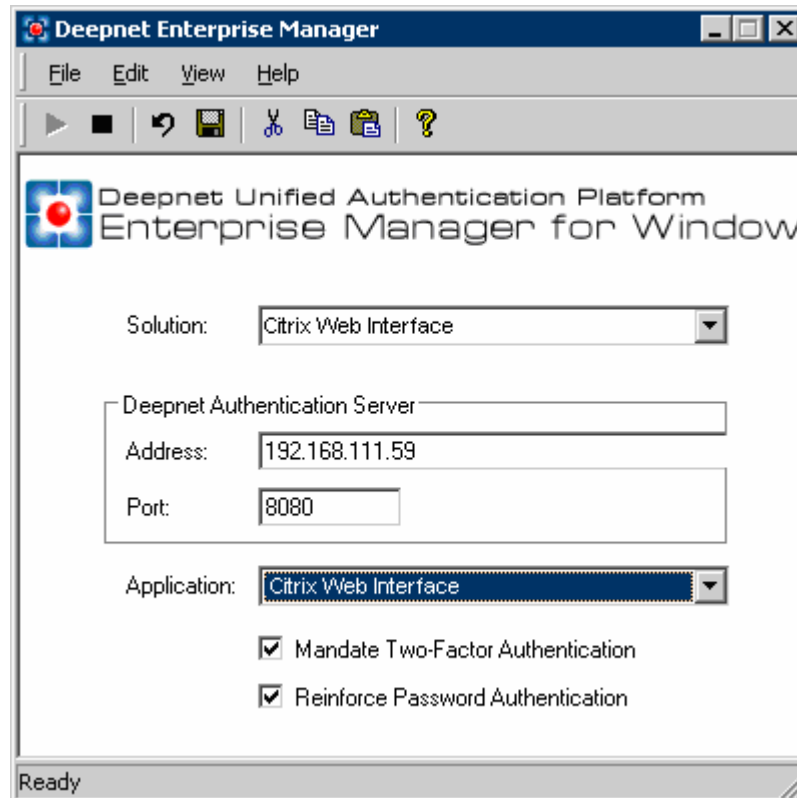
Once the application for CWI has been added to the Authentication Platform, you will then need to add to the application those users who are required to be authenticated with two-factor authentication. Each user should be allocated one or more authentication token(s) such as MobilePass and/or Mobile2x2.

Please refer to the user guide of the authentication platform for details of how to set up the application, create users and tokens.

### Configure CWI Agent

The CWI Agent needs to be configured so that it is connected to the authentication server and the application for CWI. In addition, there are options that help enforce your security policy.

The configuration tool for the CWI Agent is part of the Deepnet Enterprise Manager which is a management tool for all solutions including Windows Logon, Outlook Web Access, Citrix Web Interface and other enterprise solutions that Deepnet supports.



### Basic Configuration

1. Click the "Solution" dropdown list and select "Citrix Web Interface".
2. Enter the Address and Port of the authentication server.
3. Click the "Application" dropdown list and select the application that you have set up for Citrix Web Interface. (In the above screenshot, the sample application is named "Citrix Web Interface").

### Mandate Two-Factor Authentication

Deepnet Unified Authentication for CWI supports the concurrent use of both legacy static username/password protection and Deepnet's strong two-factor authentication, for different users within the domain. This enables a staged migration of users to two-factor authentication in your organisation, as/when convenient and appropriate.

The "Mandate Two-Factor Authentication" option applies to users who have not been added to the CWI application. If this option is **not** checked then those users who have **not** been added to the CWI application will **not** be required to authenticate themselves to access CWI. If the option is checked then everyone will be mandated to authenticate themselves with two-factor authentication.

**Note:** Users added to the CWI application are mandated to use two-factor authentication regardless whether or not the “Mandate Two-Factor Authentication” option is checked.

### **Reinforce Password Authentication**

If this option is checked then the authentication agent always verifies the static password first before asking for the second factor authentication.

If the company offers MobilePass tokens to its users, it is recommended that this option should be enabled.

If this option is enabled, you need to make sure that either your CWI application is connected to the Active Directory or each user has been given a static password (StaticPass) token in the authentication server. In latter case, the user’s login name and password have to be the same as their Citrix login name and password.

### **Save Settings**

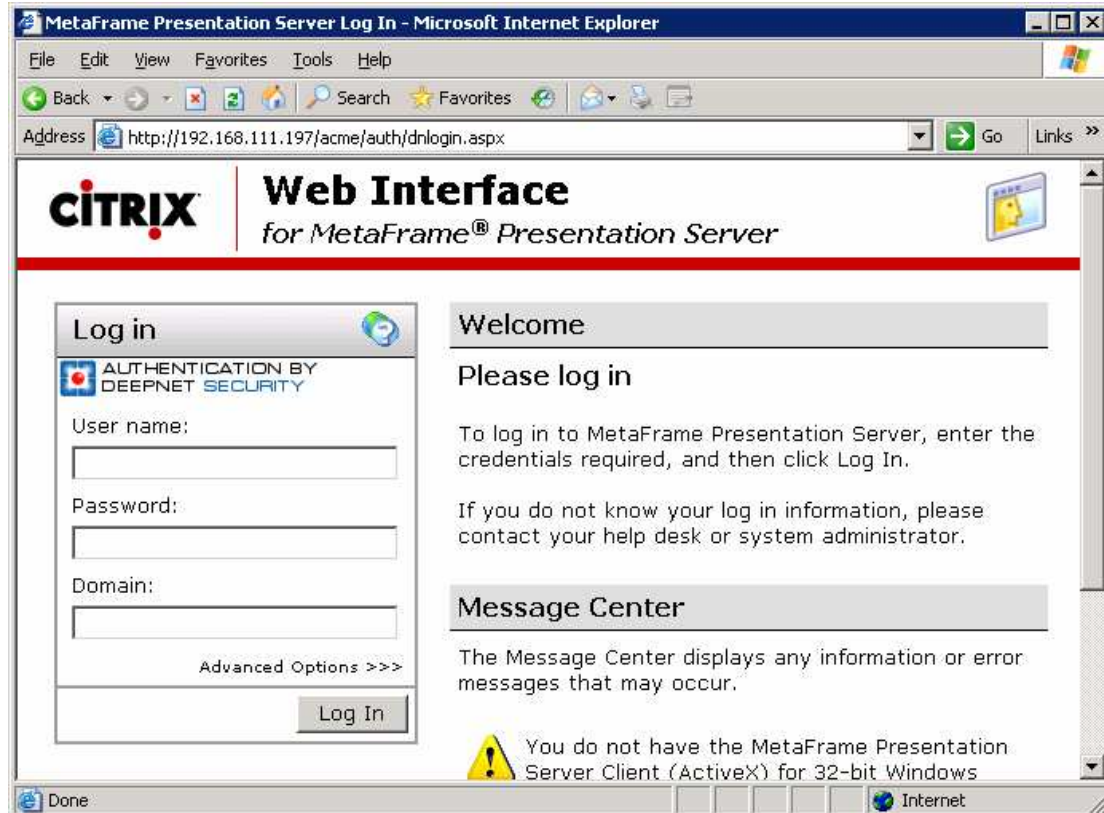
Click the “Save” button  to save your settings.

## Authentication

The process of the Two-Factor authentication for CWI logon goes through two screens: the first-factor authentication and the second-factor authentication.

### The First-Factor Authentication

The first-factor authentication is the same as the traditional static password authentication in which the user is asked to enter their user name and windows account password.



## The Second-Factor Authentication

The second-factor authentication asks the user to provide the credentials generated from their token, such as, a one-time password.

