

## **MSK Access User Control**

Version 1.0.20061121

Prepared by:  
Raymond Gallagher

## Table of Contents

MSK Access User Control.....	1
Version 1.0.20061121.....	1
Table of Contents.....	2
Executive Summary.....	3
Introduction.....	4
How does it work?.....	4
What is true two-factor authentication?.....	4
Quick Install.....	5
Step 1.....	5
Step 2.....	5
Step 3.....	5
Step 4.....	6
Step 5.....	8
Step 6.....	8
Step 7.....	8
Information you will need to get started:.....	9
IP Address.....	9
MSK Authentication Server.....	9
Certificate Request Page.....	10
Downloading MSK Access User Control.....	10
Decompress the download.....	11
Implementing the code.....	12
MSK_Access_User_Control.dll.....	12
MSK_Login.ascx.....	12
Images.....	12
Modify your login page:.....	13
Pass the Username and Password.....	13
Application setting in the Web.config file.....	13

## **Executive Summary**

The MSK Security product (Access & Identity Management) is designed to allow secure login in a web environment and to remove the possibility of non-authorized activity interfering with these processes. The Access & Identity Management product is also designed to be used as a single point of access or Single-Sign-On (SSO).

This document is designed as an introduction to MSK's Access & Identity Management product and specifically, implementation of the MSK Access User Control. This Control can be used in two modes, two-factor only or mixed mode. Mixed mode will allow your web application to keep existing single-factor usernames and passwords for some users while allowing other users to take advantage of Access & Identity Managements SSO feature. The MSK Access User Control will be transparent to users that continue to use usernames and passwords.

Access & Identity Management offers true two-factor authentication, bi-directional protection, and all the benefits of SSO.

## Introduction

The Access & Identity Management system by MSK is designed to prevent all of the common web site and consumer attack mechanisms, without the need for cumbersome or complex systems. The technology removes the username and password buffer fields from the website this simple step also removes all of the attacks against username and password buffer fields like SQL injection, password guessing, Phishing, Pharming, Man-in-the-Middle attacks...etc.

### How does it work?

The user has a small program running on their workstation called the MSK Client. This program is a stand alone executable that does not need to be installed. The MSK Client accepts the user's Passcode not the website this prevents the user from giving away their credentials to a fraudster. MSK is also true two-factor authentication one being they must know their Passcode and second they must be in possession of their MSK Client program. For added protection the MSK Client can marry itself to the user's workstation.

### What is true two-factor authentication?

Despite what some companies say there are only three possible factors for authentication something you know, something you have and something you are.

1. Something you know
  - i. Passwords, Images, Patterns, Answers to questions

Any combination of the above forms of authentications is just single-factor.

2. Something you have
  - i. Unique Client Programs, OTP Tokens, Computer, Smart Card, etc.

Any of the above systems implemented without a Passcode is still single-factor although just something you have is stronger than just something you know.

3. Something you are the strongest single factor authentication
  - i. Finger Print, Retina, DNA, etc...

## Quick Install

Information you will need to get started:

- IP Address of the office using MSK Authentication
  - Example: [127.0.0.1](#)
- URL of the MSK Authentication Server to include the [MSK\\_Response.aspx](#) page
  - Example: [https://www.msksecurity.com/Auth/MSK\\_Response.aspx](https://www.msksecurity.com/Auth/MSK_Response.aspx)
- URL to the Certificate Request Page
  - Example: <https://www.msksecurity.com/Sites/Company.aspx>
- 

### Step 1

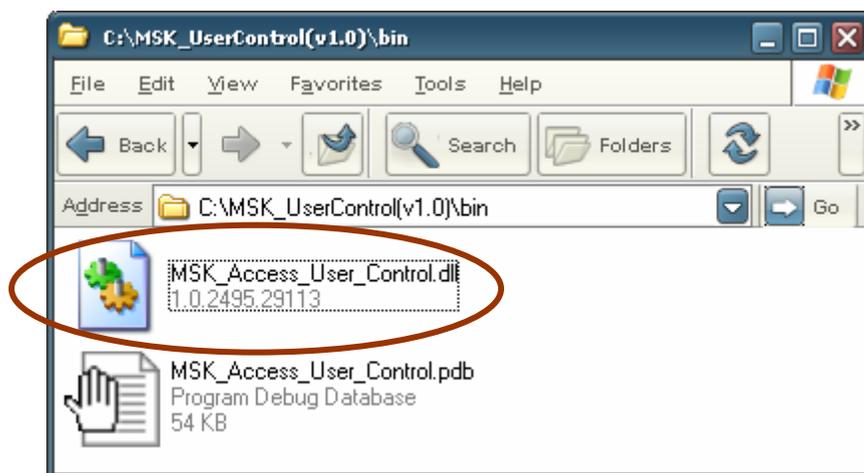
Download the MSK Access User Control from  
MSKsecurity.com → Downloads → MSK Access User Control

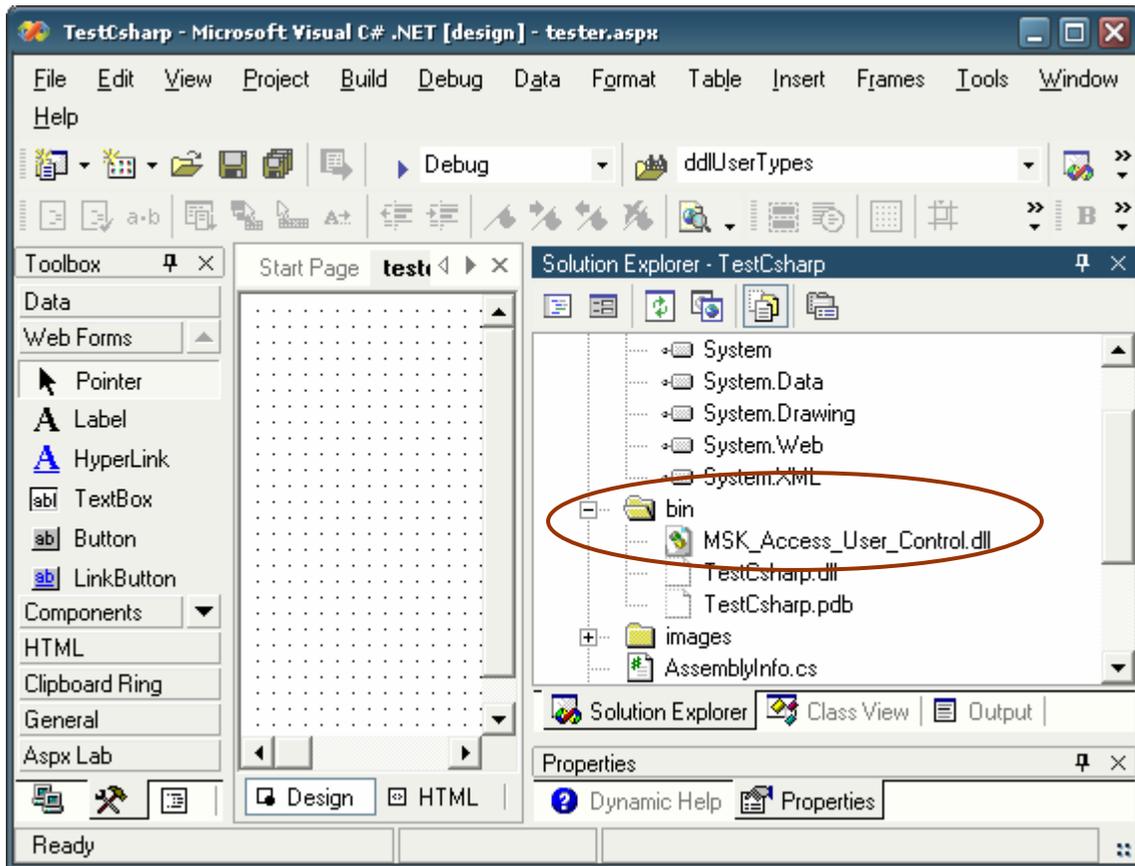
### Step 2

Unzip MSK\_UserControl(v1.0).zip  
Notice that all of the Source Code is available and can be modified to fit your needs.

### Step 3

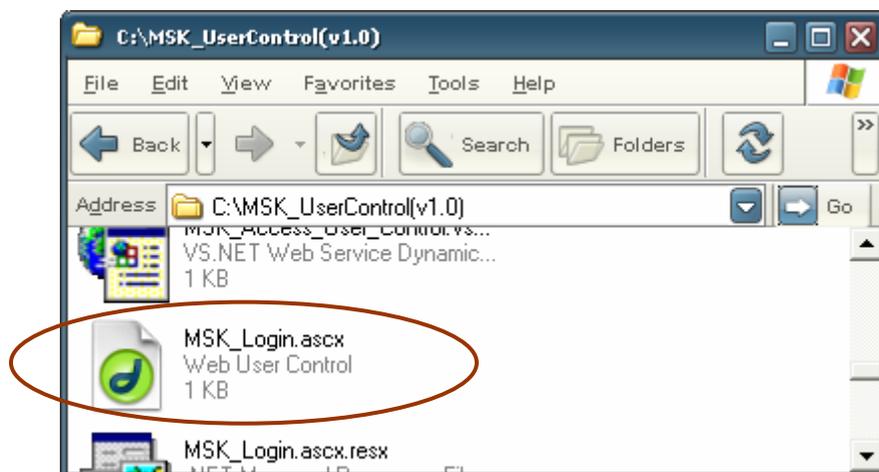
Copy the file MSK\_UserControl(v1.0)\bin\MSK\_Access\_User\_Control.dll to the bin directory of your site. In Microsoft Visual Studio 2002 you can drag and drop.



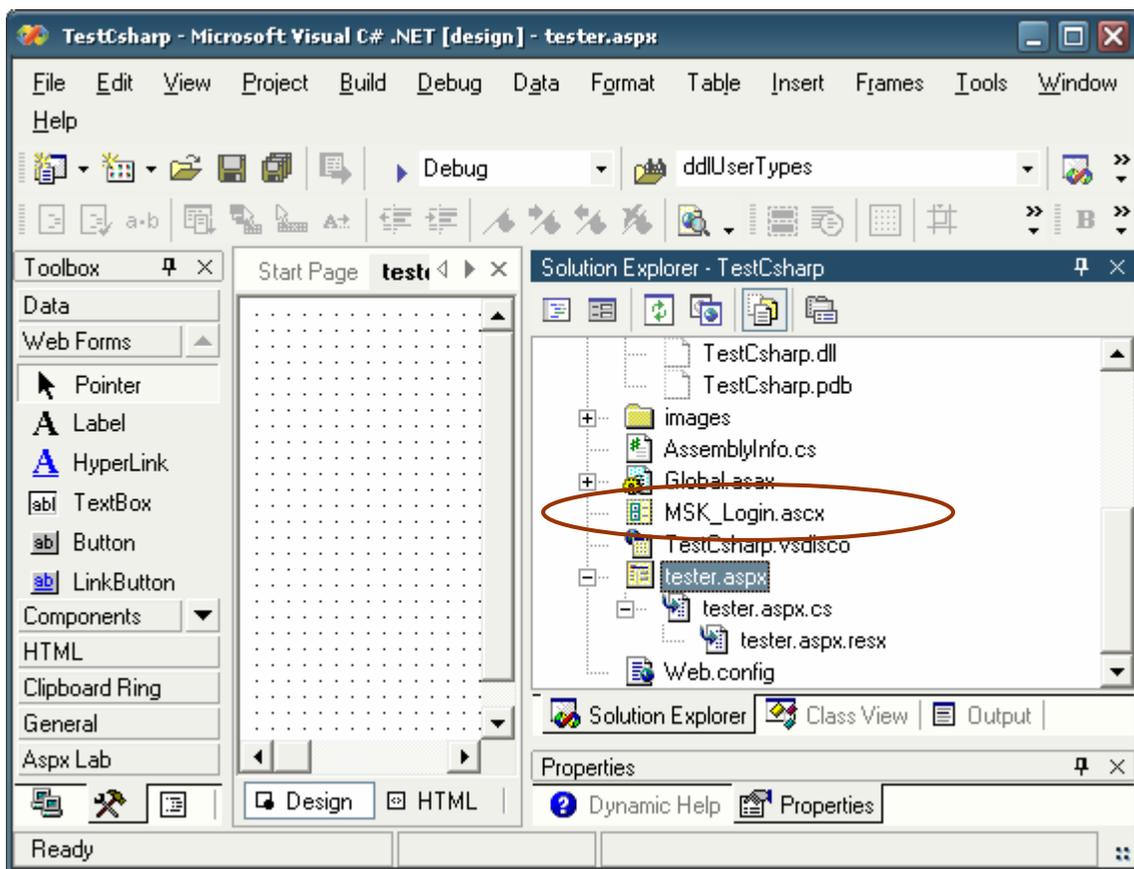
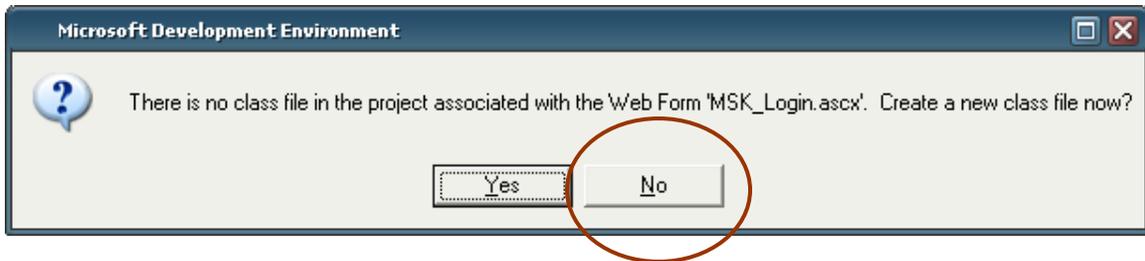


## Step 4

Copy the file MSK\_Login.ascx to the main directory of your site. In Microsoft Visual Studio 2002 you can drag and drop.



When you drag and drop this file into Microsoft Visual Studio 2002 you will get this warning. Select No.



At this point the user control is ready to be used just like any other user control. Make sure that the language for this control is set to ("vb"). Visual Studio will insert the current language for the control. Example:

```
<%@ Control Language="c#" AutoEventWireup="false" ...
```

Change to:

```
<%@ Control Language="vb" AutoEventWireup="false" ...
```

The control uses image buttons so don't forget to copy over the images.

Drag and drop the "images folder" into your site if you don't already have an "images folder" other wise drag and drop the images into your "images folder."

## Step 5

Drag and drop the MSK\_Login.ascx User Control into your login page

## Step 6

Modify your login page to only show the username and password buffer fields for non MSK Users

Example:

```
<uc1:MSK_Login id="MSK_Login1" runat="server"></uc1:MSK_Login><br>  
<% if not Session("MSK_User") then %>...
```

Username and password buffer fields

```
<% end if %>
```

The session variable `Session("MSK_User")` is used to determine if a user is an MSK user its value will be True or False.

The session variable `Session("username")` is used for the Username.  
The session variable `Session("password")` is used for the Password.

## Step 7

Modify the Web.config file with information obtained from the implementers of the MSK Authentication Server

```
<appSettings>  
  <!-- IP address for users who have implemented MSK Access &  
  Identity Management -->  
  <add key="MSK_IP" value="127.0.0.1" />  
  <!-- Get Response from MSK Auth Server (did the user authenticate  
  and who authenticated) -->  
  <add key="MSK_Response_URL"  
  value="https://www.msksecurity.com/auth/MSK_Response.aspx" />  
  <!-- Request One Time Certificate from MSK Auth Server -->  
  <add key="MSK_Request_URL"  
  value="https://www.msksecurity.com/Sites/Company.aspx" />  
  <!-- User Control MSK_Mode values are "MIXED" and "TWO_FACTOR".  
  Mixed mode allows usernames and passwords to be used. With this  
  mode you must set an IP address for "MSK_IP", only users from  
  this address will even see the MSK Login button. "TWO_FACTOR"  
  mode is for complete integration default setting is "MIXED" any  
  incorrect value will return the default; MSK might change this  
  behavior in future versions -->
```

```
<add key="MSK_Mode" value="MIXED" />  
</appSettings>
```

Now you have completed the process.

## Information you will need to get started:

### ***IP Address***

You will need the IP Address/Addresses of MSK Users this is how the control will determine if users are MSK Users or Users who are still using usernames and passwords.

A single IP Address or many can be used

```
<add key="MSK_IP" value="127.0.0.1" />
```

For multiple IP's use a comma to separate the list

```
<add key="MSK_IP" value="127.0.0.1,127.0.0.4,127.0.0.3" />
```

For "TWO\_FACTOR" mode use

```
<add key="MSK_IP" value="" />
```

### ***MSK Authentication Server***

You will need the URL of the MSK Authentication Server being used.

```
<add key="MSK_Response_URL"  
value="https://www.msksecurity.com/Auth/MSK_Response.aspx" />
```

This URL is where the control will check if the user has logged. If the user has logged in then the control will get the username and password so that your system will know who is logging in and assign appropriate user rights.

NOTE: THIS URL SHOULD BE A SECURE CONNECTION. SSL OR TLS

## Certificate Request Page

The MSK Authentication server issues onetime certificates on the fly for every login. You will need the URL of the Certificate Request Page being used by the implementers of the MSK Authentication Server. The certificate request page is the webpage that has the server identification information.

```
<add key="MSK_Request_URL"  
value="https://www.msksecurity.com/Sites/Company.aspx" />
```

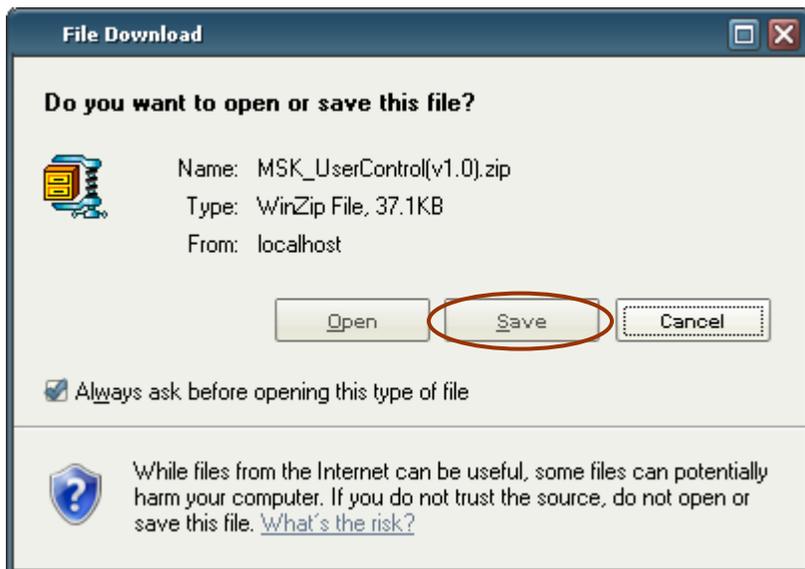
The MSK Access User Control will check to see if it has a certificate if not then it will redirect to this page. This page will then issue the onetime certificate.

NOTE: THIS URL SHOULD BE A SECURE CONNECTION. SSL OR TLS

## Downloading MSK Access User Control

The control can be downloaded for free from our website. To insure that you download the most current version go to <http://www.msksecurity.com> then navigate to **Downloads** → **MSK Access User Control**





The current version of the control when this document was released is [MSK\\_UserControl\(v1.0\).zip](#)

## Decompress the download

[MSK\\_UserControl\(v1.0\).zip](#) contains the source code and project files from which the control was compiled.

```
\MSK_UserControl(v1.0)
  \bin
    MSK_Access_User_Control.dll
    MSK_Access_User_Control.pdb
  \images
    btnLogoFailedReset.gif
    btnLogoLogin.gif
    MSK_logo_2_small.gif
  \objects
    CertPolicy.vb
    HttpPOST.vb
  AssemblyInfo.vb
  Global.asax
  Global.asax.resx
  Global.asax.vb
  MSK_Access_User_Control.sln
  MSK_Access_User_Control.vbproj
  MSK_Access_User_Control.vbproj.webinfo
```

```
MSK_Access_User_Control.vsdisco
MSK_Login.ascx
MSK_Login.ascx.resx
MSK_Login.ascx.vb
Styles.css
test.aspx
test.aspx.resx
test.aspx.vb
Web.config
```

The important files are

```
\\MSK_UserControl(v1.0)\bin\MSK_Access_User_Control.dll and
\\MSK_UserControl(v1.0)\ MSK_Login.ascx
```

## Implementing the code

### MSK\_Access\_User\_Control.dll

By copying the file [MSK\\_UserControl\(v1.0\)\bin\MSK\\_Access\\_User\\_Control.dll](#) into the bin directory of your site your site will have access to the objects in the control. In Microsoft Visual Studio 2002 you can drag and drop.

### MSK\_Login.ascx

Copy the file MSK\_Login.ascx to the main directory of your site. Again in Microsoft Visual Studio 2002 you can drag and drop. Then you can drag and drop the control onto the login page of your website. Visual Studio 2002 will automatically assign the control to the main "dll" file for your site you may need to change this. The first line of this file should read:

```
<%@ Control Language="vb" AutoEventWireup="false"
Codebehind="MSK_Login.ascx.vb"
Inherits="MSK_Access_User_Control.MSK_Login"
TargetSchema="http://schemas.microsoft.com/intellisense/ie5" %>
```

### Images

The following image files are supplied with the control

```
btnLogoLogin.gif      → This is the Login button
MSK_logo_2_small.gif  → This is the MSK Security's Logo
```

The images are called from the relative folder \images\ since all of the source code is available the control can be modified to use any images you want to better match the look and feel of your site.

### **Modify your login page:**

#### **Pass the Username and Password**

Modify your login page to only show the username and password buffer fields for non MSK Users. Make sure that the MSK\_Login user control appears before you check the session variable `Session("MSK_User")`. The control is self contained in a table.

Example:

```
<ucl:MSK_Login id="MSK_Login1" runat="server"></ucl:MSK_Login><br>
```

The username and password are pulled from the MSK Authentication Server. End users do not need to know the username and password for this system. Easier for end users and a More Secure system

```
(Your company Username Variable) = Session("username")  
(Your company Password Variable) = Session("password")
```

```
<% if not Session("MSK_User") then %>...
```

Username and password buffer fields

```
<% end if %>
```

The session variable `Session("MSK_User")` is used to determine if a user is an MSK user its value will be True or False.

### **Application setting in the Web.config file**

Modify the Web.config file with information obtained from the implementers of the MSK Authentication Server. Details for these parameters are outlined in the section called **Information you will need to get started:**

There are only four settings and they all are prefixed with "MSK\_" so they should not interfere with existing settings.

```
<appSettings>
  <!-- IP address for users who have implemented MSK Access &
  Identity Management -->
  <add key="MSK_IP" value="127.0.0.1" />
  <!-- Get Response from MSK Auth Server (did the user authenticate
  and who authenticated) -->
  <add key="MSK_Response_URL"
  value="https://www.msksecurity.com/auth/MSK_Response.aspx" />
  <!-- Request One Time Certificate from MSK Auth Server -->
  <add key="MSK_Request_URL"
  value="https://www.msksecurity.com/Sites/Company.aspx" />
  <!-- User Control MSK_Mode values are "MIXED" and "TWO_FACTOR".
  Mixed mode allows usernames and passwords to be used. With this
  mode you must set an IP address for "MSK_IP", only users from
  this address will even see the MSK Login button. "TWO_FACTOR"
  mode is for complete integration default setting is "MIXED" any
  incorrect value will return the default; MSK might change this
  behavior in future versions -->
  <add key="MSK_Mode" value="MIXED" />
</appSettings>
```