Authentication. Evolved.

CUSTOM LOGON EXPERIENCE

INSTALLATION AND USER GUIDE

June 12th 2015

Version 1.11 June 2015

Table of Contents

1. DOCUMENTATION

1.1. Version Control

#ID	Owner
1.00	Chris Dubravs, Software Engineer
1.10	Ahmad Ali Iqbal, Software Developer
1.11	Chris Dubravs, Software Engineer

1.2. Document Definitions & Acronyms.

Acronym/Term /Notation	Description
SID	Security ID. A Unique code that represents either a user or group of a computer or domain.
RDP	Remote Desktop Protocol is used to connect to the remote machine.

1.3. Purpose Summary

The purpose of the following document is to provide the steps required to install and uninstall Mi-Token's custom desktop logon experience. It also contains troubleshooting steps and optional steps to make the installation experience require little to no user action.

1.4. File Description

File Name	Description
MiToken_CredentialProvider_xxxx.exe	Where 'xxxx' is a 4 digit version number. It contains the installer for both 32 and 64 bit systems. Can optionally have an Auto Configuration file attached to it to allow silent installation.
API Setup.exe	This utility allows configuration of the Credential Provider including setting up the default API servers, user bypasses, credential screen filters and advanced security and diagnostic options.

API Tester.exe	This utility allows verification that the API configuration is correct. However it does not support testing bypass code authentication.

2. NORMAL INSTALLATION PROCEDURE

1. If the Mi-Token API has not been previously installed, install the Mi-Token API (*Mi-Token API Service_Xbit.exe where X is either 64 or 32*) and ensure that its certificate is bound with IIS Server. Take a note of the API server's name or IP address as it will be required in later steps during credential provider configuration.

   Note: See the API installation guide for further details.

2. Copy the latest Mi-Token Credential Provider Installer exe file onto the machine you would like to install Mi-Token's Custom Desktop Login.
3. Run the installer. The Installer will now identify if the system is a 32 or 64 bit system and run the appropriate Setup program.

   Note: Do not close down the Installer prompt while the Setup program is running.

4. Read and accept the Mi-Token End User License Agreement (EULA), then press install.
5. At the end of installation and just before finishing, Mi-Token API Configuration Tool will pop up.
6. Add the Servers you setup in Step 1
   1. Click Add on the Authentication page
   2. Type in either the Servers IP address (e.g. 127.0.0.1) or Hostname (e.g. localhost) and click Add.
   3. It will first validate and then add the IP or Hostname.
   4. Repeat steps 6.1 to 6.3 for all Mi-Token API servers
7. *Optional but Recommended:* You can now add SID specific bypass code if you wish to. You can also add a common code for all users.

   Note: It is recommended to set up a bypass code, at least initially, in case user OTPs fail to authenticate due to an invalid configuration, user are still able to login with this bypass code.

   1. Click Configure Bypass. The Bypass Configuration dialogue will open up.
   2. Select 'Add…'
   3. Either click 'Select User / Group' or check 'All Users'
   4. Type a Bypass Code in the textbox.
   5. Click OK.
   6. Repeat steps 7.2 to 7.5 until you have all the user bypasses you would like.
   7. Click OK
8. Optional: You can configure various Filter Mode configurations such as enabling/disabling CP on local machine login or for remote connectivity connection types. You can also configure what options should be shown on credential page for each connection type.
   1. Click on Configure Filter Modes.

Note: If you would like Mi-Token Credential Provider to be enabled only on remote connections to the machine, you can check the RDP Only checkbox next to the Configure Filter Modes button and then skip steps 8.2 to 8.4.

2. Select the type of connection who's filter you would like to change. The Filter settings pane will change to indicate what the current filter on that connection type is
3. Select the new filter type you would like for this connection.
4. Click OK.

9. *Optional:* You can now configure advanced security options
    1. Click 'Configure security options'
    2. If you want the custom logon experience to occur when booting in safe mode, check 'Force credential providers in safe mode'.

        Note 1: This only works for Windows 7 or Windows Server 2008.

        Note 2: It is highly recommended you test that the custom logon experience works on this machine before checking this box. Otherwise you may end up in a situation where it is impossible to logon to this machine.
    3. If you are having trouble with Mi-Token's custom logon experience you may check the 'Enable Debug Logging' checkbox to turn on verbose logging.

        Note 1: Under normal usage this will not be needed.

        Note 2: The checkboxes Enable Verbose Logging and Enable Sensitive Logging should not be checked unless directed to by Mi-Token support.
    4. If you want Dynamic Passwords, check the Enable Dynamic Passwords checkbox.

        Note: Please read the section on Dynamic Passwords in this document before checking this box. Also we suggest you discuss with Mi-Token support before checking this box due to issues that could arise from enabling it.
10. Click 'Close'

    Note 1: If no API Servers were setup you will be asked to add at least one to the list.

    Note 2: If no user bypasses were configured you will be warned and asked if you would like to continue.
11. Click 'Finish' on the Setup window.
12. By default, Desktop login installs on 'C:\Program Files\Mi-Token\Mi-Token Desktop Login' from where you can access the 'API Setup.exe' and 'API Tester.exe' utilities if you need to at later stage.

3. UNINSTALLING

1. Open a command prompt
2. Navigate to the folder Installer.exe is in
3. Type “Installer.exe -U”
4. Press Enter
5. Mi-Token Custom Logon Experience will now uninstall.

OR

1. Click on ‘Start’ button and navigate to Control Panel
2. Click on ‘Uninstall a program under ‘Programs’ category
3. Double click ‘Mi-Token Desktop Login’ to uninstall the software.

4. USAGE

4.1. Local Machine Logon

4.1.1. Windows XP/2003

When logging in, the user will be prompted for their username and password. After validating the combination of these two credentials, the user will be asked for their OTP. Access to the system will only be granted if OTP is validated for a token which was assigned to that user. If bypass code for a particular user or for all users is configured that can also be used in replacement of OTP.

4.1.2. Windows Vista/7/2008

When logging in, the user will be prompted for their username, password and Mi-Token OTP. Access to the system will only be granted if combination of username, password and OTP are validated associated with the user. If bypass code for a particular user or for all users is configured that can also be used in replacement of OTP.

4.2. Remote Logon

4.2.1. Windows XP/2003

When try to login remotely through RDP session, the user will be prompted for their username and password. After validating the combination of these two credentials, the user will be asked for their OTP. Access to the system will only be granted if OTP is validated for a token which was assigned to that user. If bypass code for a particular user or for all users is configured that can also be used in replacement of OTP.

4.2.2. Windows Vista/7/2008

When connecting from the remote PC through RDP, the user will be prompted to supply their username and password. Once a valid username and password combination has been supplied the user will be connected to the remote PC. The user will then be asked just for their Mi-Token OTP to finish logging onto the PC.

4.3. Safe Mode

4.3.1. Windows XP/2003

It will be same as a normal logon.

4.3.2. Windows Vista/7/2008

If 'Force Credential Providers in safe Mode' during the installation (Step 2.9.2) was checked it will be the same as with a local machine logon, otherwise the default Windows Credential Provider will be used.

4.4. Dynamic Password

You can configure the credential provider to use only one field either for password or OTP by setting the Dynamic Password option. This option is useful when an organization want to allow login to the system by OTP only if a token is assigned to a user otherwise AD users can login with standard AD password.

Note: Users cannot login with the AD password if a token is assigned to the user.

It is important to know that the Dynamic Password option resets the AD user password to some random value which is used to perform AD authentication by the

credential provider. It keeps changing the password each time the user successfully authenticates with OTP. This is to ensure that once users are configured with tokens, their password should not be any more vulnerable to the authentication mechanism. Therefore the user must change his AD password manually at later stage if user needed to use it for any other reason.

4.4.1. Configuration

The option to enable Dynamic Passwords can be found on the Security Options screen of the API Setup tool.

4.5. Centralized Administration

Mi-Token Credential Provider supports centralized administration of bypass codes. To enable Centralized bypass code administration the option will need to be enabled on a Mi-Token API server. From there the bypass codes will be synced between the server and the client whenever a valid OTP token is authenticated.

5. TROUBLESHOOTING

Question: I am trying to test the API configuration using Tester tool but it fails to authenticate with the bypass code.

Answer: The API Tester tool cannot authenticate with bypass codes, it can only be used for testing the valid OTP from a token assigned to a user.

Question: A user has a token assigned and I verified that it is working with the Radius tester but it is not authenticating with Tester tool from Windows logon.

Answer: Please ensure that API Server address is correct and Mi-Token API server is up and running. Sometimes firewalls also block sending the request to API server, ensuring this also helps resolving the issue.

Question: I have just recently installed windows desktop login but I am not sure if I have configured correctly. Now I am afraid if I logoff may not be able to login.

Answer: You can configure the Filter mode so that you can always log on with the default credential provider. To do this, choose the option 'Disable Nothing' in the filter settings pane. While this setting is active both the windows default credential provider as well as the Mi-Token Credential Provider will be available for you to use to login.

Question: While installing the Mi-Token Credential Provider my machine locked and now I have the Mi-Token Credential Provider asking me for an OTP to login. However I haven't setup any API Servers, how do I log in?

Answer: The Mi-Token Credential Provider lock screen is active as soon as it is installed; however OTP values are not checked until the API Setup screen has been completed. In this scenario leaving the OTP field blank and just typing in the username and password will work fine.

6. ADVANCED OPTIONS

6.1. Adding Auto configuration option to the installer

It is possible to add auto configuration options to the installer. Adding these options will have the following effect on the logon experience:

- You will no longer be prompted during the install process to agree to the EULA
- You will no longer be prompted during the install process to add API Servers or SID based bypasses
- The install process will add API Servers and SID based bypasses that are contained in the auto configuration file during install.
- The install process will require no user interaction once Install.exe is started

Auto configuration files contain the following information

- A list of default API Servers to use (IP Address / Hostname)
- A list of SIDs and their bypass codes (encrypted)
- Weather to turn Debug logging on by default or not.

To add an Auto configuration file to the installer:

1. Run API Autoconfig.exe.
   Optional: Run it as Administrator so you do not have to worry about the UAC prompts in step 9 and 12.
2. *Optional*: If you already have an Auto configuration file you would like to use the settings of click 'Load Autoconfig File', Navigate to the file and click OK.
3. Follow steps 7 and 8 of the Install Process for adding API Servers and SID based bypass codes, taking note that SID based bypasses are accessed via the tab bar at the top.
4. *Optional:* If you would like Debug Logging on by default check 'Default Debug Logging'
5. *Optional:* To save the Autoconfig file without adding it to an installer click 'Create Autonconfig File'
   Note: You need to save an Autoconfig file to add it to an installer so if you are just about to add it to an installer this step is not required.
6. Click "Add Config File to Installer".
7. Select a location to save the Autoconfig file to and click OK.
8. Select Installer.exe as the installation application to use.
9. If required accept the UAC prompt.
10. If the installer you selected in Step 7 already had an Auto Configuration file attached to it you will now be warned and asked if you would like to overwrite the old configuration
11. Select where you would like to save the new installer.
    Note: It **cannot** have the same name and location as the Installer chosen in Step 7.
12. If required accept the UAC prompt.
13. You will be informed that the file was either successfully imported or the reason why the import failed.
14. You may now use the file selected in Step 11 as the installer on any PC that you would like these default settings.