What is nFactor

nFactor authentication enables dynamic authentication flows based on the user profile. In some cases, these could be simple flows to be intuitive to the user. In other cases, they could be coupled with securing active directory or other authentication servers.

nFactor Concepts, Entities, Terminology

Login schema	nFactor decouples the 'view', the user interface, with the 'model' that is the runtime handling. nFactor's view is defined by lotgin schema'. Login schema is an entity that defines what user sees and specifies how to extract the data from user.
Policy label	A policy label is a collection of policies. It is a construct not alien to Citrix ADC's policy infrastructure. Policy label defines an authentication factor. That is, it contains all the policies necessary to determine whether credentials from user are satisfied.
Virtual server label	In Citrix ADC's advanced policy infrastructure, a virtual server is also an implicit policy label. That's because virtual server can also be bound with more than one policy. However, a virtual server is special because it is the entry point for client traffic and can take policies of a different type.
Next factor	Whenever a policy is bound to a virtual server or a policy label, it can be specified with next factor. Next factor determines what should be done if a given authentication succeeds. If there is no next factor, that concludes authentication process for that user.
No-Auth policy	nFactor introduces a special kind of built-in policy called NO_AUTHN. NO_AUTHN policy always returns success as authentication result.
Passthrough factor/label	Passthrough factor implies that authentication, authorization, and auditing subsystem should not go back to user to get credential set for that factor. Instead, it is a hint for authentication, authorization, and auditing to continue with already obtained credentials

nFactor Other Information

nFactor authentication framework provides the flexibility of adding customizations to make the logon interface more intuitive for rich user experience. You can add custom login labels, custom login credentials, customizing UI displays and so on.

All factors created by admin in the nFactor flow are retained for any future use.

Citrix recommends that you must not use policy label names such as, 'root' and ' as suffix and '_db_' as prefix.

You can only add or edit the decision block through Citrix ADC GUI. There is no option to configure the decision block from CLI command.

Citrix recommends modifying the nFactor flows using nFactor Flows page only.

Starting in Citrix ADC release 13.0 build 36.27, nFactor configuration through GUI is simplified by using the nFactor Visualizer.

How Does it Work?

Imagine a user requesting access to an application that requires user credentials. As is the case in Citrix ADC deployments, the request arrives at the Citrix ADC appliance through a traffic management virtual server (in this case, a load balancing virtual server). Since the user must provide authentication credentials, the load balancing virtual server redirects the request to the authentication virtual server, which does the following:

1 Checks to determine whether any login schema policies are associated with the authentication virtual server.

- If yes, the user is presented the login form associated with the login schema policy with the highest priority that evaluates to true.

- If no, the default login form is presented to the user.

  Note: The default login schema files are available in the /nsconfig/loginschema/LoginSchema/ directory of the Citrix ADC appliance. Citrix recommends that you copy these files to the /nsconfig/loginschema/ directory before using them, so that changes made to the files are preserved post reboot.

2 The authentication policies that are associated with the authentication virtual server are evaluated. For the policies that are evaluated to true, the actions are executed in order of priority until one of the actions succeeds.

3 The policy label that is associated as the next factor is invoked.

4 The authentication policies that are associated with the authentication policy label are evaluated. For the policies that are evaluated to true, the actions are executed in order of priority until one of the actions succeeds.

5 The policy label that is associated as the next factor is invoked.

6 Steps 3 to 5 are performed repetitively until all the configured next factors are executed.

nFactor Visualizer for Simplified Configuation

Starting from Citrix ADC release 13.0 build 36.27, nFactor configuration through GUI is simplified by using the nFactor Visualizer. The nFactor Visualizer helps admins add multiple factors without losing track of each factor. The group of factors that are built in the flow are displayed in one place. Admins can add authentication success and failure paths separately. After creating the flow, admins have to bind the nFactor flow to an authentication virtual server.

Note: All factors created by admin in the nFactor flow are retained for any future use.

Previously, nFactor configuration was cumbersome wherein the admins had to visit many pages to configure it. If a change was required, the admins had to revisit the configured sections each time. Also, there was no option to view the complete configuration in one place.

To Launch the nFactor visualizer:
Navigate to Security→AAA- Application Traffic→nFactor Visualizer

Customizing First Factor View for End-Users

1 Create a loginschema

2 Create a loginschema policy

3 Create an AAA virtual server

4 Bind the loginschema policy to the AAA virtual server

High Level Configuration Steps

Configure any number of authentication factors.

Base the selection of the next factor on the result of executing the previous factor.

Customize the login interface. For example, you can customize the label names, error messages, and help text.

Extract user group information without doing authentication.

Configure pass-through for an authentication factor. No explicit login interaction is required for that factor.

Configure the order in which different types of authentication are applied. Any of the authentication mechanisms that are supported on the Citrix ADC appliance can be configured as any factor of the nFactor authentication setup. These factors are executed in the order in which they are configured.

Configure the Citrix ADC to proceed to an authentication factor that must be executed when authentication fails. To do so, you configure another authentication policy with the exact same condition, but with the next highest priority and with the action set to "NO_AUTH". You must also configure the next factor, which must specify the alternative authentication mechanism to apply.