TrustSec 1.99 Deployment Note: FlexAuth Order, Priority, and Failed Authentication

Flexible Authentication (FlexAuth) is a set of features that allows IT administrators to configure the sequence and priority of 802.1X, MAC-Auth Bypass (MAB), and switch-based web authentication (local webauth). Before changing the default order and priority of these authentication methods, it is important to understand the potential consequences of these changes. If MAB is configured to run before 802.1X, then all devices in the network will attempt to authenticate using MAB. This could result in significant additional authentication traffic on the network. Also, the interactions with other FlexAuth features, which are described in this deployment note, must be considered.

Case 1: MAB First and Higher Priority

Currently, by default, authentication priority changes with the order. So if you change the order to put MAB before 802.1X, then by default, any device that passes MAB will never be allowed to do 802.1X. In this case, if you want a device to perform 802.1X, then it must fail MAB. Consequently, its MAC address must not be in the databases that are checked for MAB nor can you have a policy that allows unknown MACs to succeed MAB, such as for dynamic Guest VLAN assignment.

In this case, you cannot use MAB to remediate known devices that fail 802.1X, such as an. employee PC with expired certificate. Therefore, for 802.1X failures use the configuration: **event fail action next-method**, and configure the next-method as local web-auth. If **event fail next-method** is configured and local web-auth is not configured, the switch will try to authenticate the device again using MAB. The device will keep failing MAB and 802.1X and will not gain access.

If local web-auth is not an option, use the configuration **event fail action authorize vlan** to put devices that fail 802.1X in the auth-fail VLAN. If a device fails 802.1X and is placed into the auth-fail VLAN, to get out of the auth-fail VLAN, one of the following must occur:

- Reauthentication from the switch
- EAPoL-Logoff/EAPoL-from the supplicant
- Link down/up event

If you perform reauthentication, reauthentication will always go back to the first method, which in this case is MAB.

Note Some platforms may support the Cisco AVpair (termination-action-modifier=1) that instructs the switch to retry only the last authentication method.

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

In summary, remember three things when MAB comes before 802.1X in both order and priority:

- Make sure that all devices that perform 802.1X are not in the MAC database and the configured policy never returns Access-Accept for unknown MACs. 802.1X devices must fail MAB if they are to perform 802.1X. As a consequence, many MAB failure records will be generated in the course of normal operation.
- Only use event fail action next-method if the next-method is local web-auth.
- If the next-method is not local web-auth, the only option for granting access after 802.1X failures is event fail action authorize vlan (the auth-fail VLAN).

Case 2: MAB First in Order but Higher Priority Assigned to 801.1X

If you change the order so that MAB comes before 802.1X and change the default priority so that 802.1X has higher priority than MAB, then every device in the network will still undergo MAB,. However, devices that pass MAB can subsequently authenticate via 802.1X. This enables a scenario where devices can get partial access to be assigned an IP address or begin a PXE boot, and so forth, after successful authentication via MAB and then get complete access after a successful 802.1X authentication. In this case, you can have 802.1X devices in your MAB database.

Pay attention to what happens if a device fails 802.1X after a successful MAB. First, the device will have temporary network access between the time MAB succeeds and 802.1X fails. What happens next depends on the configured event-fail behavior. If local web-auth is not configured, then the switch will return to the first method (MAB) after the configured interval (**dot1x timeout quiet-period**). MAB will succeed, the device will again have temporary access until and unless the supplicant tries to authenticate again. This behavior is supplicant-dependent. Some supplicants will stop attempting 802.1X after a certain number of failed attempts and some will continue indefinitely. If the supplicant stops attempting 802.1X altogether, the device will eventually end up with MAB-authorized access. If the supplicant continues to attempt 802.1X, the device will have intermittent access as it cycles between successful MAB and failed 802.1X.

If **event fail next-method** and local web-auth are both configured and if the supplicant retries 802.1X during or after web-auth, then 802.1X will not start again, regardless of the status of the web authentication. This is because after 802.1X fails, local web-auth ignore EAPoL-Starts from the supplicant.

The only way to deterministically assign access to devices that fail 802.1X after passing MAB is to use the **event fail authorize vlan**. configuration After failing 802.1X, the device will be placed in the auth-fail VLAN and no other methods will be attempted. Because EAPoL-Starts are ignored in the auth-fail VLAN, supplicant behavior will not change the authorization state of the port. Again, the only way to get out of auth-fail VLAN is reauthentication from the switch, EAPoL-Logoff/EAPoL-from the supplicant, or a link down/up event.

In summary, remember three things when MAB comes first in order, but 802.1X has priority:

- Devices that perform 802.1X can be in the MAC database.
- Using event fail next-method with dot1x timeout quiet-period without local web-auth can lead to unpredictable behavior and intermittent network access, with MAB cycling to 802.1X failure.
- For truly deterministic behavior after 802.1X failure and successful MAB, use event fail authorize vlan (the auth-fail VLAN) or local web-auth.