Propagate Object Configuration Changes

For supported software information, click here.

You can propagate changes made to an object's configuration to any entity that uses that object. If more than one version of an object uses the object you update, you can choose to which versions the updated object is propagated.

For example, you may have created an access control rule called Scan-Web-Emails.v1. You then used this rule in an access control policy (Default-Security-Policy). The access control policy is used in a Security subprofile (Default-Security-Profile), and the Security subprofile is used in two master profile (Hub-Master-Profile and Spoke-Master-Profile). All objects belong to the parent tenant ACME.

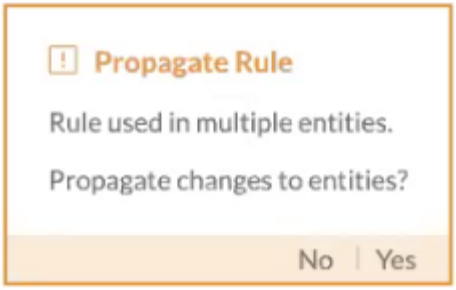
In addition, you have created three versions of the Default-Security-Policy that use the Scan-Web-Emails rule, four versions of the Default-Security-Profile subprofile that use Default-Security-Policy, and multiple versions of the two master profiles that use the Default-Security-Profile subprofile, Hub-Master-Profile and Spoke-Master-Profile.

You have now used the access control rule Scan-Web-Emails.v1 in the following objects:

- ACME (tenant)
  - Scan-Web-Emails.v1 (Access control rule)
    - Default-Security-Policy.v1 (Access control policy)
      - Default-Security-Profile.v1 (Security subprofile)
    - Default-Security-Policy.v2 (Access control policy)
      - Default-Security-Profile.v2 (Security subprofile)
    - Default-Security-Policy.v3 (Access control policy)
      - Default-Security-Profile.v3 (Security subprofile)
      - Default-Security-Profile.v4 (Security subprofile)
        - Hub-Master-Profile.v5 (Standard master profile)
        - Hub-Master-Profile.v6 (Standard master profile)
        - Hub-Master-Profile.v7 (Standard master profile)
      - Spoke-Master-Profile.v16 (Basic master profile)
      - Spoke-Master-Profile.v17 (Basic master profile)
      - Spoke-Master-Profile.v18 (Basic master profile)

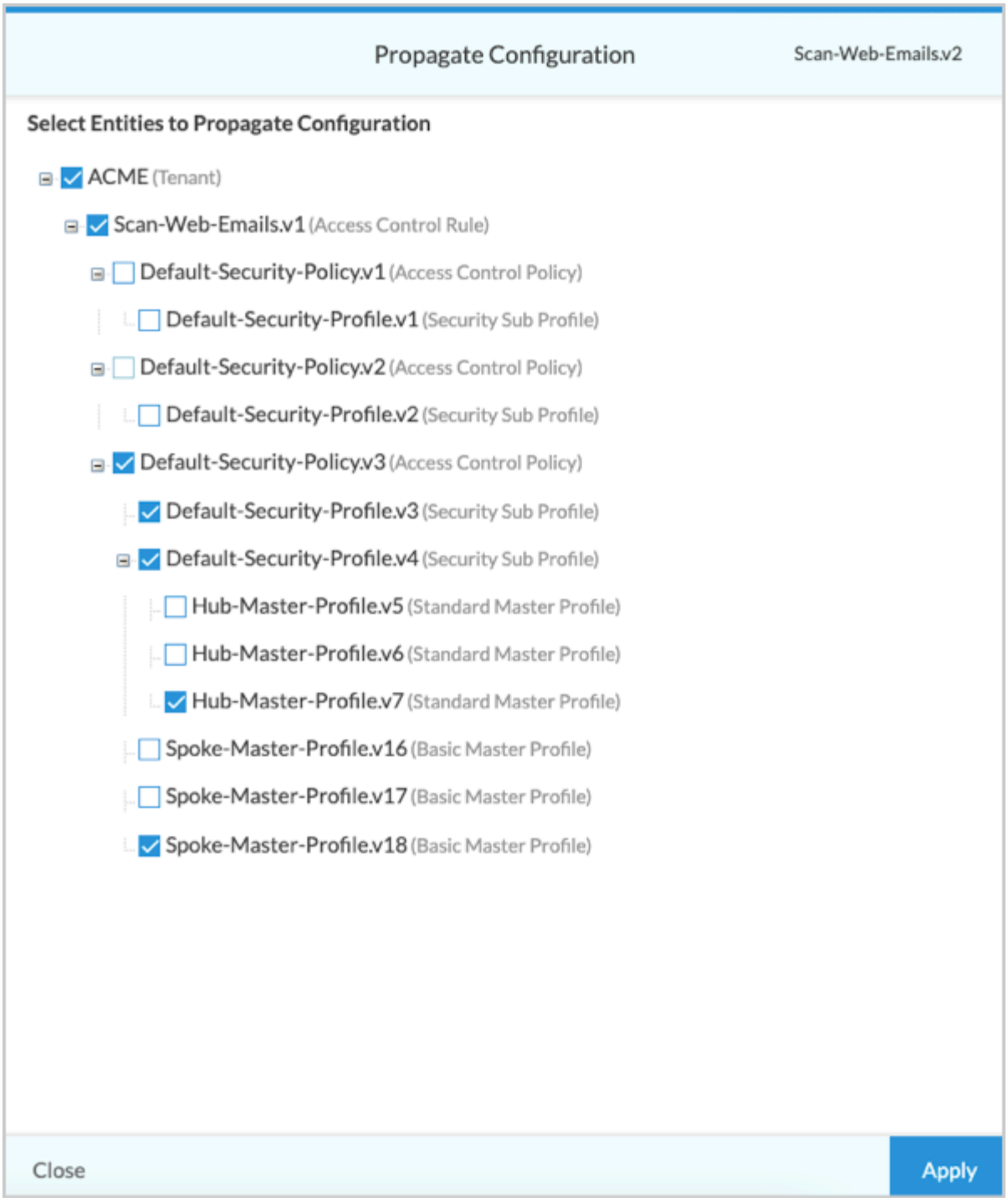
To propagate a change to the Scan-Web-Emails.v1 rule:

1. Go to Configure Profiles > Profile Elements > Rules > Security > Access Control.
2. Select Scan-Web-Emails.v1.
3. Make a change to the configuration of Scan-Web-Emails.v1.
4. Save the change. Scan-Web-Emails.v1 is saved as a new version, Scan-Web-Emails.v2, and the Propagate Rule popup window displays.



Note: In Release 10.2.1 and later, object versions apply across tenants. If another tenant had previously modified Scan-Web-Emails.v1 and saved it as Scan-Web-Emails.v2, the version you just created would be named Scan-Web-Emails.v3. For more information, see Object Versioning.

5. Click Yes to propagate Scan-Web-Emails.v2. The Propagate Configuration screen displays. Select one or more objects to which Scan-Web-Emails.v2 will be propagated. If you select the topmost object, ACME, then all child objects of ACME are selected.



6. Click Apply. The updated rule is propagated to the selected objects.

Supported Software Information

Releases 10.2.1 and later support all content described in this article.

Additional Information

Preserve Director Node-Level Configuration Changes
Propagate Configuration Changes to Appliances
View References to Objects in the Configuration Hierarchies