Qualys 8.10.1 Release Notes

This new release of the Qualys Cloud Suite of Security and Compliance Applications includes improvements to Vulnerability Management and Policy Compliance.

Qualys Cloud Platform

Hide Users Outside the Business Unit
New Scanner Role Extended Permissions
Minimum Password Length Increased
Improved Password Tip

Qualys Policy Compliance (PC/SCAP)

Enhancement to File Integrity Monitoring
Mac OS X 10.12 Technology Supported for UDCs

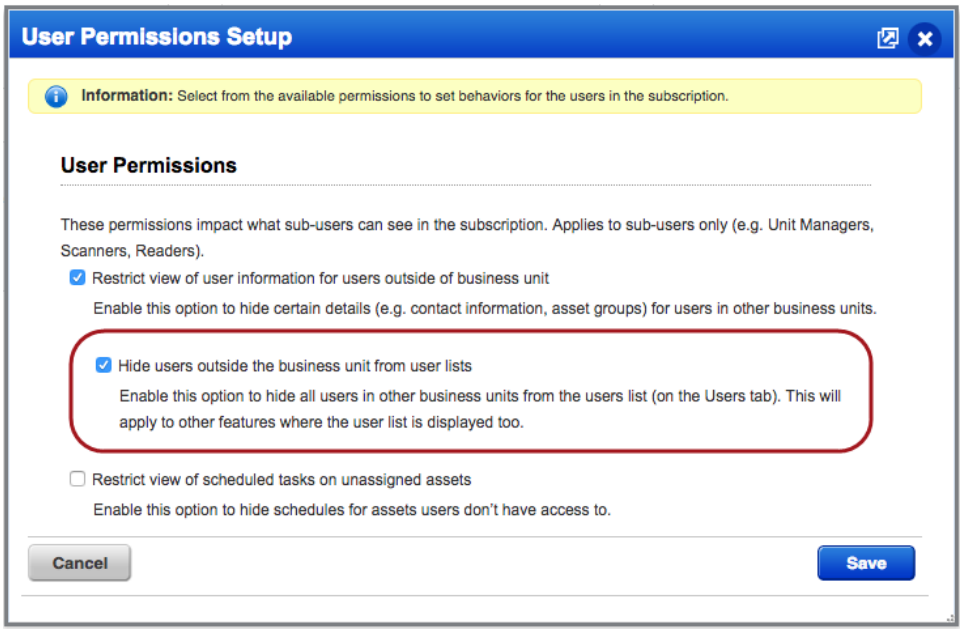
Qualys 8.10.1 brings you many more Improvements and updates! Learn more

Qualys Cloud Platform

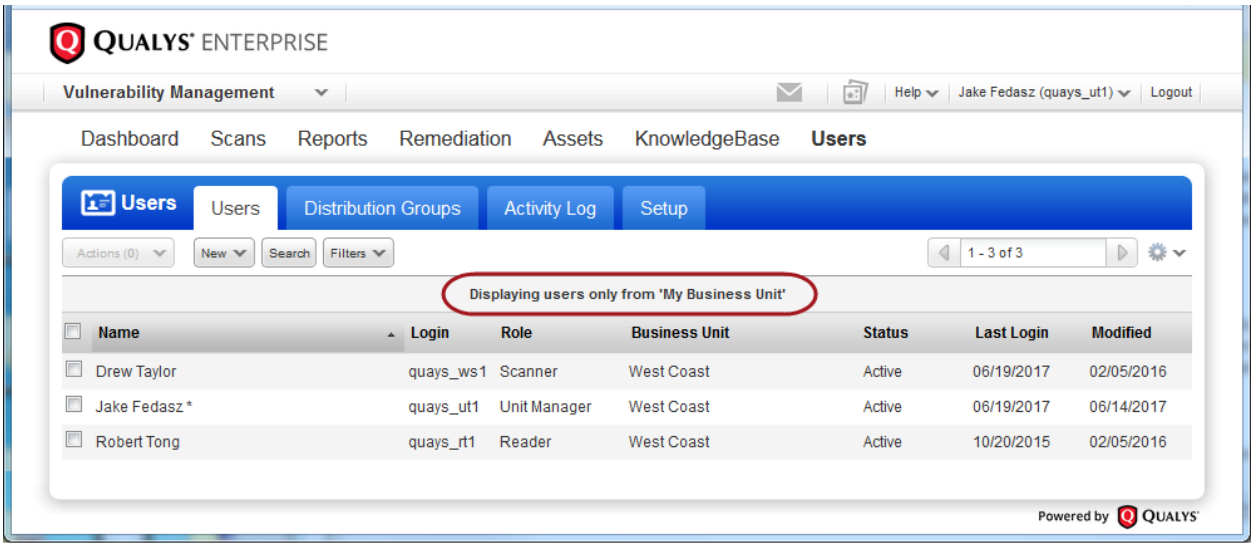
Hide Users Outside the Business Unit

This release introduces a new user permission that impacts what sub-users scan see in the subscription. When enabled, sub-users (e.g. Unit Managers, Scanners, Readers) will only see the users in their own business unit. Users outside of their business unit will be hidden from view.

A Manager can set this up by going to Users > Setup > User Permissions. Select these options together:
- Restrict view of user information for users outside of business unit
- Hide users outside the business unit from user lists



In this example, the logged in user is part of the West Coast business unit and is only able to see users in the same business unit. The message above the list (circled in red) lets you know the list has been filtered.



We'll also hide users from user lists in other areas of the UI. Here are some examples:

- The Filters menu on the Users list will not include these filters for sub-users: Hierarchy Chart and My Business Unit. Also, the Search option will not show the Business Unit drop-down for sub-users.

- When creating a distribution group (Users > Distribution Groups), sub-users can only select users in the same business unit. Tip – You can still manually add email addresses for users outside of your unit.

- When reassigning remediation tickets (Remediation > Tickets), sub-users can only select users in the same business unit.

New Scanner Role Extended Permissions

Your subscription may now be configured to allow users with a Scanner user role to be granted these extended permissions:

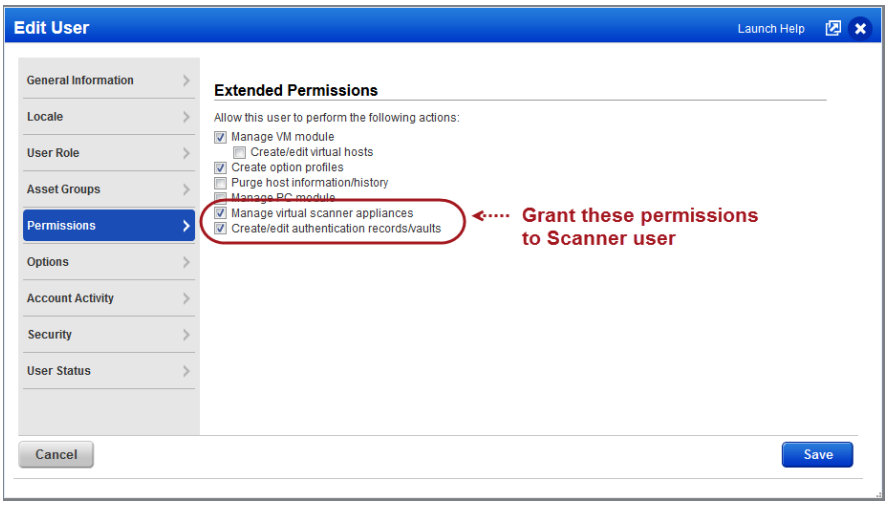
- Manage virtual scanner appliances. When granted, this allows the user to create, edit and delete virtual scanner appliances from the UI and API.

- Create/edit authentication records/vaults. When granted, this allows the user to create and edit authentication records and vaults from the UI and API.

Note that these permissions may already be granted to Unit Manager accounts.

How to grant a user extended permissions

These permissions may be granted on a per user basis by a Manager or Unit Manager (with the same permission). Simply edit the user's account from the Qualys UI by going to the Users list and choosing Edit from the Quick Actions menu. Then choose permissions on the Permissions tab.

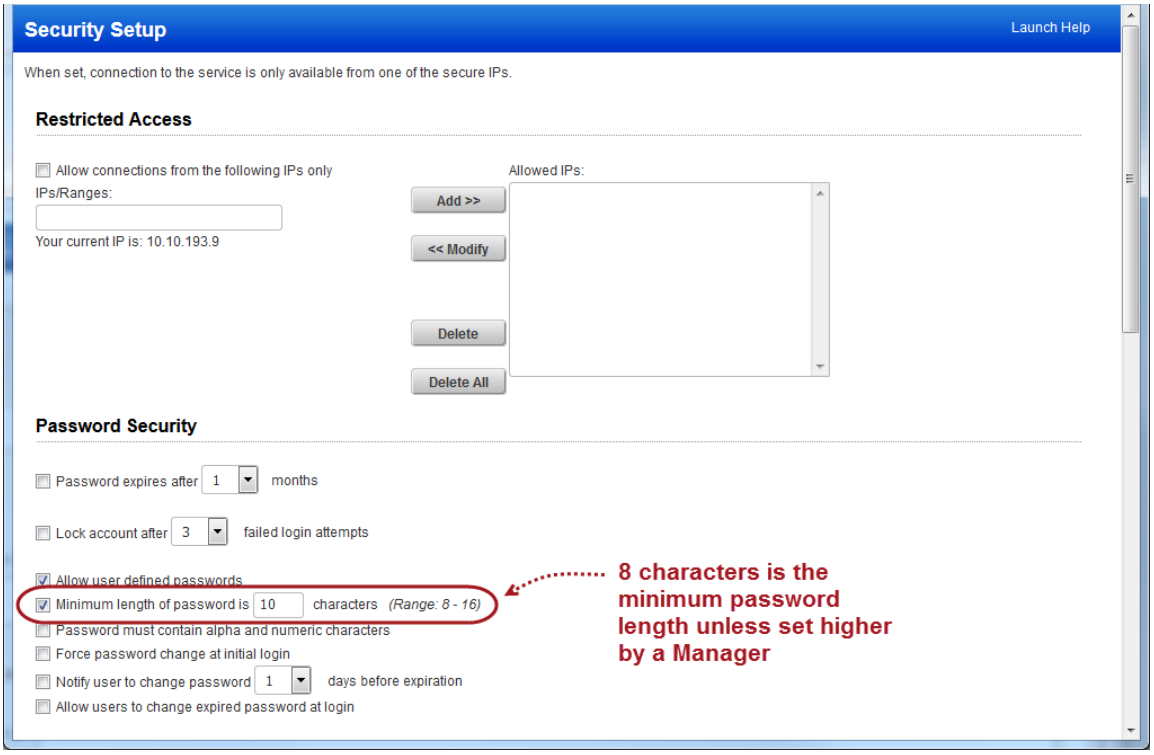


Not seeing these permissions for Scanner users?

Your subscription must be configured to allow Scanner users to be granted these additional permissions. Please contact your Technical Account Manager or Support to have this enabled for you. Once enabled, you'll be able to grant these permissions to any Scanner user in your subscription.

Minimum Password Length Increased

For improved security, the minimum password length for all user accounts has been increased from 6 to 8 characters. This is the minimum password length enforced by Qualys. A Manager can set a higher minimum (up to 16 characters) by going to Users > Setup > Security. The next time you change your password it must meet the new minimum length requirement.



Improved Password Tip

When you go through the Forgot Password workflow, one of the password tips on the Change Password screen is to include special characters. The special characters were listed inside parenthesis and were comma separated, and this was confusing to some customers. We've removed the commas and parenthesis since these characters are not valid for your password.

The password tip now reads:
Include at least one of these special characters: ! @ # $ % - / _ + \

Qualys Policy Compliance (PC)

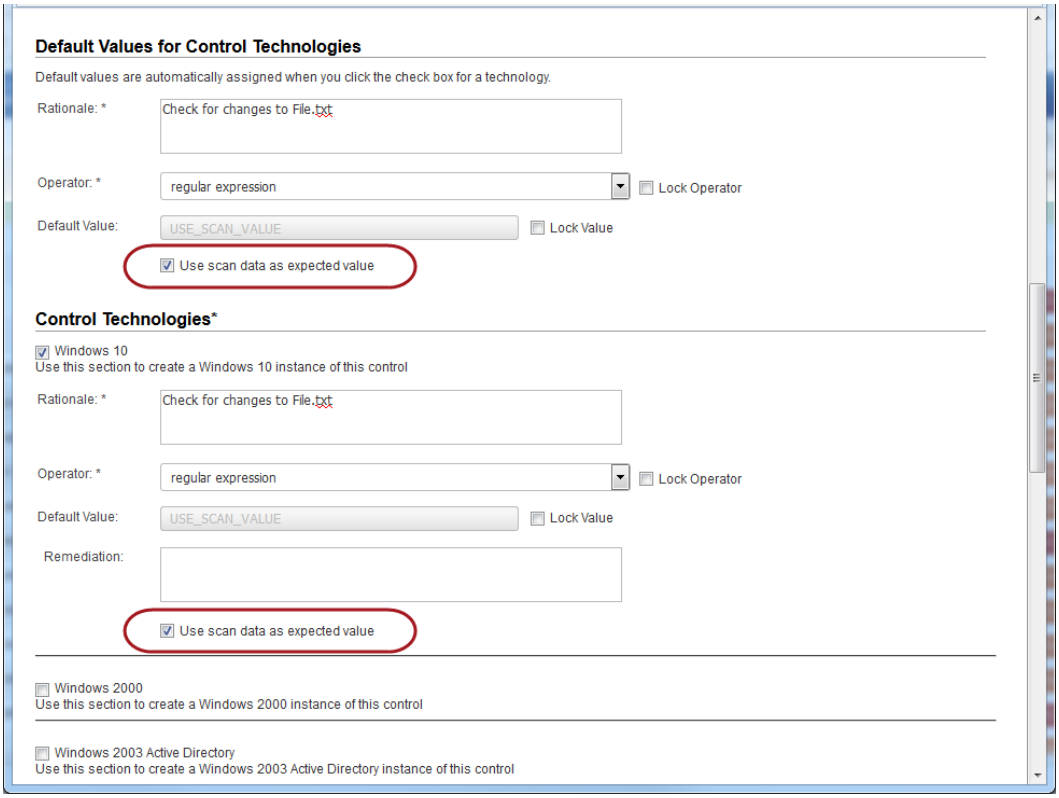
Enhancement to File Integrity Monitoring

Using Qualys PC you can perform file integrity monitoring based on user defined file integrity checks. A file integrity check is a user defined control that checks for changes to a user-specified file. With this release you're no longer required to manually set the default expected value for each file integrity check. Now you can pick the "Use scan data as expected value" option in the UDC and we'll set the expected value for you based on the actual value returned by the scan.

It's a 2-step process to set this up:

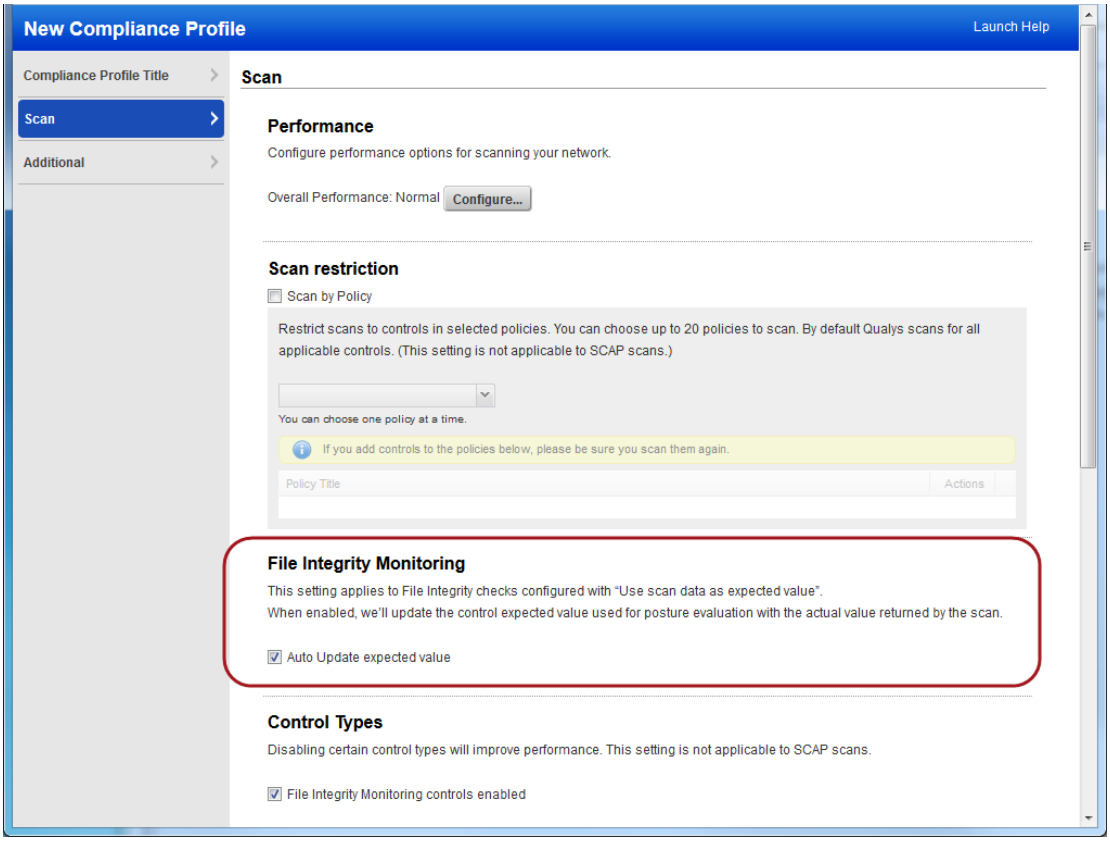
1 - Configure your file integrity check to use scan data

Go to PC > Policies > Controls > New > Control, and choose File Integrity Check for Windows or Unix. Select "Use scan data as expected value" for individual technologies or make it the default for all technologies. When selected, you'll see USE_SCAN_VALUE in the Default Value field.



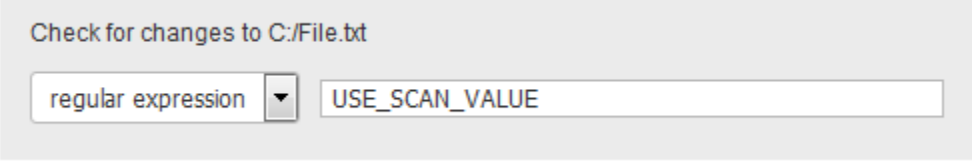
2 - Enable this option in your compliance profile

Go to PC > Scans > Option Profiles. Create a new profile or edit an existing one. On the Scan tab, select "Auto Update expected value" under File Integrity Monitoring. You must also select "File Integrity Monitoring controls enabled" like in previous releases to include these controls in your scan.

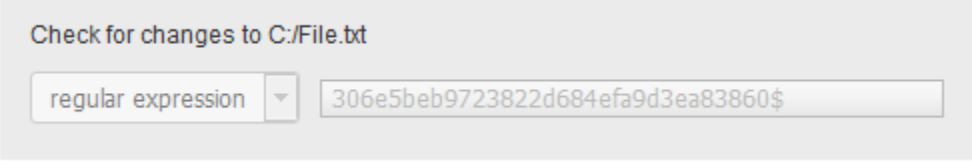


How it works

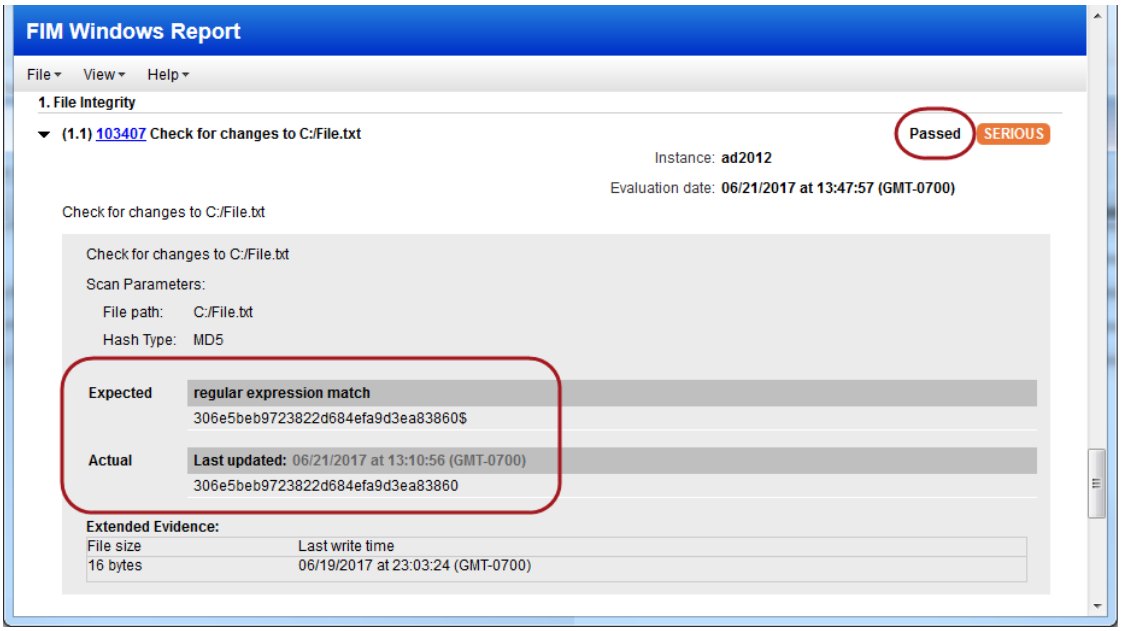
When you first add a file integrity control to a policy you'll see USE_SCAN_VALUE as the expected value for the control.



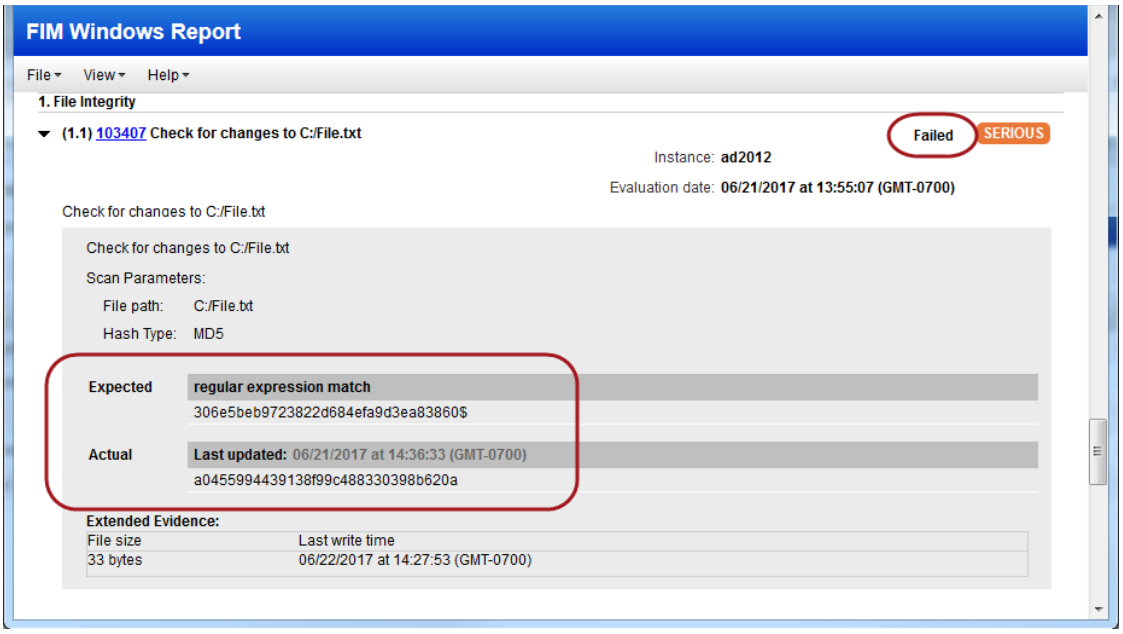
After your first scan, we'll update the expected value with the actual file hash returned by the scan.



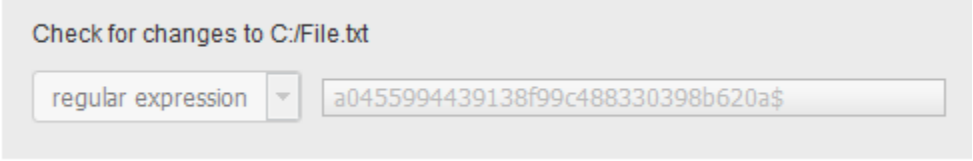
You'll see a posture of Passed for this control in your compliance reports, and you'll continue to see a posture of Passed as long as the file does not change.



If the file changes a different file hash will be returned by the scan and you'll see a posture of Failed in your reports. This is because the expected value and the actual value no longer match.

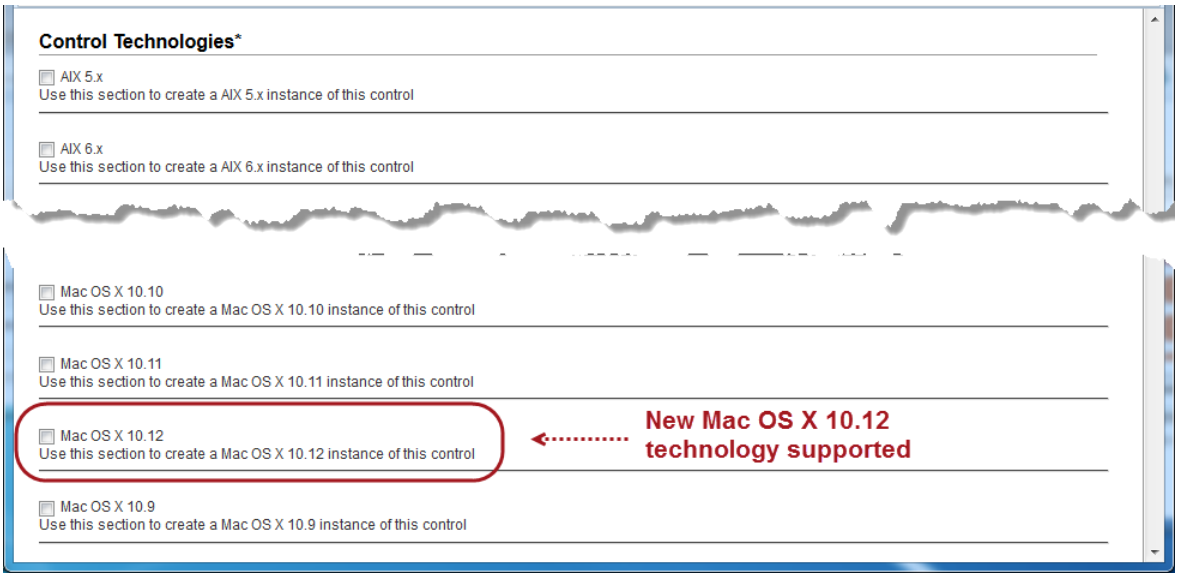


Launch another scan with "Auto Update expected value" enabled in your compliance profile and we'll automatically update the expected value for your control in the policy with the value returned by the most recent scan. Now the new value will be used for posture evaluation.

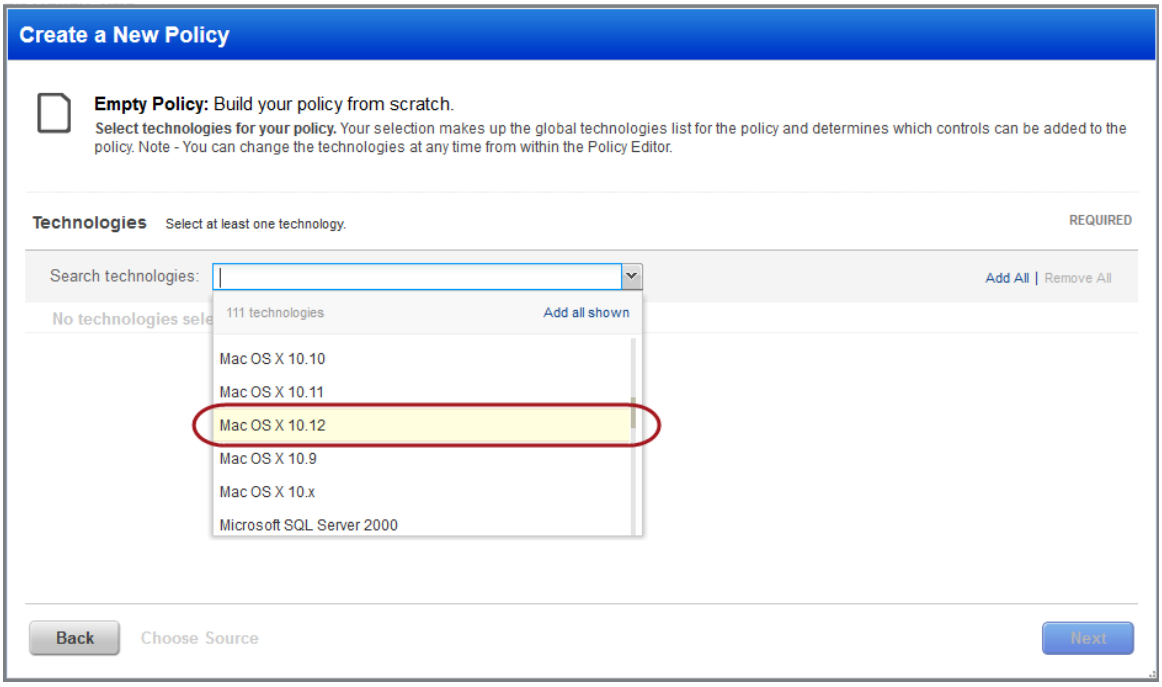


Mac OS X 10.12 Technology Supported for UDCs

Want to create a UDC for Mac OS X 10.12? Go to Policies > Controls > New > Control, and select any of the Unix control types. Scroll down to the Control Technologies section to provide a rationale statement and expected value for each technology you're interested in.



You'll also see Mac OS X 10.12 in the technologies list when creating a new policy.



Issues Addressed

- Fixed an issue where we weren't showing the Scanner Appliance on the Scan Status page (under General Information > Scan Overview).
- We will now correctly calculate the Next Launch date for a Scheduled Scan when the Occurrence setting is changed from Relaunch on Finish to Daily, Weekly or Monthly.
- (Applies to users with IPv6 Scanning enabled) Fixed an issue where scan results fetched using the API (api/2.0/fo/scan/?action=fetch) showed the mapped IPv4 addresses instead of the scanned IPv6 addresses.
- Fixed an issue where some users saw extra IP addresses (specifically DNS tracked hosts) listed on the Host Assets page that were no longer in their subscription.
- Fixed an issue which caused an error when attempting to download a completed report.
- Fixed an issue with duplicate entries on the Users data list.
- In HTTP Authentication records, we now allow "<" and ">" characters as part of the password.
- Corrected the error message that appears on the Login page when your IP address is not in the list of IPs allowed to connect to the service.
- Fixed a typo in the Operator drop-down of the File Content Check UDC. Changed "regular expression" to "regular expression".
- Updated the Cisco Authentication help to state that Cisco ACS version 5.8 is not supported.
- Updated online help template file whutils.js to remove comments. This change does not impact how online help is presented to users, it impacts template file included in the help packaging.