Sensitive data stripping

Preface

Starting with version 1.9.0, Unimus supports stripping sensitive data from backups of devices.
When this feature is enabled, passwords, pre-shared-keys, and other sensitive data will not be stored in backups of devices.

This can be enabled in "Backups > Configuration > Sensitive data stripping".
You can enable stripping sensitive data globally ("Default sensitive data stripping policy"), or per-Tag.

Per-Tag policy always over-rides the default policy for devices that the Tag applies to.
If a single device belongs to Tags that specify both the "Never strip" and the "Always strip" policy, the more secure option ("Always strip") will be applied.

Always check for desired behavior

When using this feature, **always verify if all sensitive data is properly being stripped**.
Also verify if data which should be present is not getting stripped when it should not be.

Supported devices

Currently, sensitive data stripping is supported on these devices:

```
Cisco ASA
Cisco IOS
Cisco IOS XR
Cisco Nexus
Cisco NXOS (generic NXOS)
```

If a backup is ran on a device which is not yet supported and it's configured for sensitive data stripping, the backup job will fail.
(fail reason will be "SENSITIVE_DATA_STRIPPING_ERROR")

We are periodically adding support for more devices to the above list.
If you want to use sensitive data stripping with any devices not listed above, **please let us know**.