SteelCloud®

AUTOMATING STIG & CIS COMPLIANCE

Reference Guide

for

ConfigOS™ Foundry

Version 1.09

September 2021

www.steelcloud.com **20110 Ashbrook Place, Ashburn, VA 20147** **703-674-5500**

SteelCloud
AUTOMATING STIG & CIS COMPLIANCE

Reference Guide for ConfigOS Foundry

Contents

A. Using this Guide

Welcome to the Reference Guide for the ConfigOS Foundry. ConfigOS is a patented technology for authoring remediation of endpoint security policy. ConfigOS is an integral part of ongoing security policy validation, maintenance, and remediation. This Guide was developed to help the user create secure custom policy Signatures using the ConfigOS Foundry. Once created, the ConfigOS Signature can be used with the ConfigOS Client Manager to validate/remediate security policy.

☑ ***Key Concept*** *– Please review the ConfigOS Foundry End User License Agreement (EULA) in the Appendix prior to installation.*

B. ConfigOS Description

When IT and IA professionals look to accelerate the RMF/ATO accreditation process while maintaining ongoing STIG/policy compliance, the question always comes up "is there an automation technology that can really help?" To answer that question SteelCloud developed ConfigOS to both, quickly harden policy controls around an application environment, and keep systems in compliance with the latest security policies at the lowest possible effort and cost. ConfigOS is a started task and is only run when the user wants to scan and remediate system policies and configurations.

For government customers, or those organizations that want to implement/maintain STIG or CIS-compliant systems, SteelCloud has a number of valuable Signatures. ConfigOS Signatures are machine-executable XML versions of the DISA STIG and CIS policies.

Available Signatures

- Windows 2008 R2, 2012, & 2016 – *for non-Domain systems*
- Windows 2008 R2, 2012, & 2016 – *for Domain systems*
- Windows 7, 8, 10
- Windows Firewall
- Microsoft Office 10, 13 & 16
- Internet Explorer 10 & 11
- Domain Controller (DC) – *Windows 2008, 2012 & 2016*
- IIS
- SQL Server 2012
- Red Hat Linux 5, 6, & 7
- CENTOS Linux
- Un-harden all Windows Components
- ACAS/Nessus Harden/Un-harden – *STIG*
- Chrome
- Others – *upon client request*

The remainder of this guide will step you through how to use the ConfigOS Foundry to edit signatures provided by SteelCloud to create your own secure signatures.

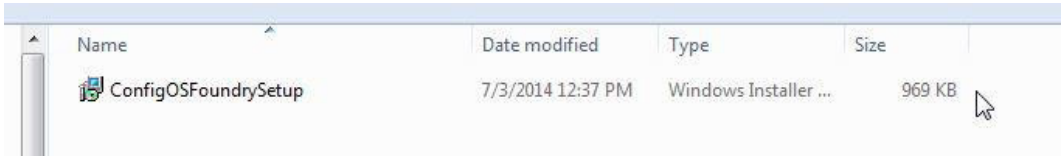
C. ConfigOS Foundry Overview

The ConfigOS Foundry ("Foundry") is a simple straight-forward software application that creates secure Signature Containers that are used by the ConfigOS Client to update policy and validate configurations. The Foundry has the following functions:

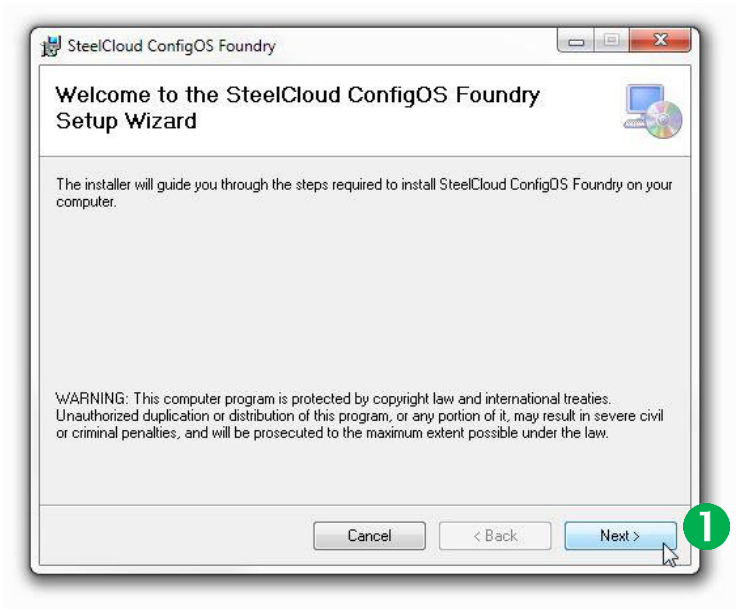
1. Generates ConfigOS Foundry and Client Keys
2. Allows the user to select the XML Policy and Control files to be included in the Signature Container
3. Allows the user to select additional files to be included in the Signature Container that might include policy documents, work instructions, etc.
4. The Foundry encrypts the individual Policy and Control XML files using the Foundry-generated keys
5. The Foundry zips and hashes the user selected files into a single Signature Container that is named by the Foundry user.

D. Installing the ConfigOS Foundry

Locate and **Click** on the ConfigOS Foundry Set-up file (see below).

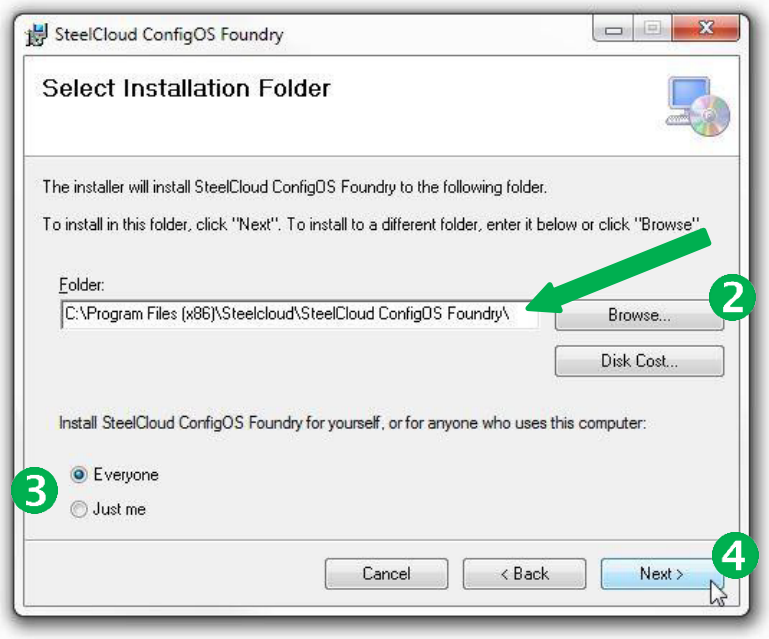


The ConfigOS Foundry Set-up Wizard will start and you will see the following screen:



1 Select "***Next***" to begin the installation of the Foundry.

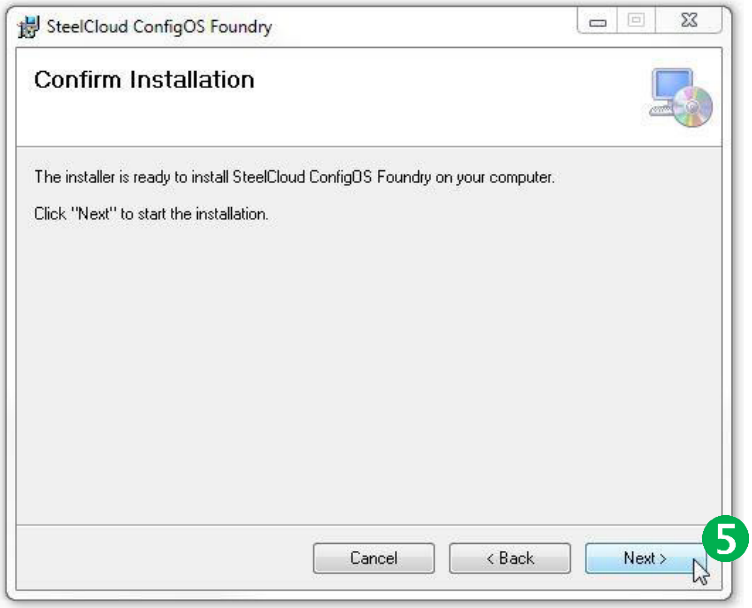
The screen below allows the user to select what folder to install the Foundry program.



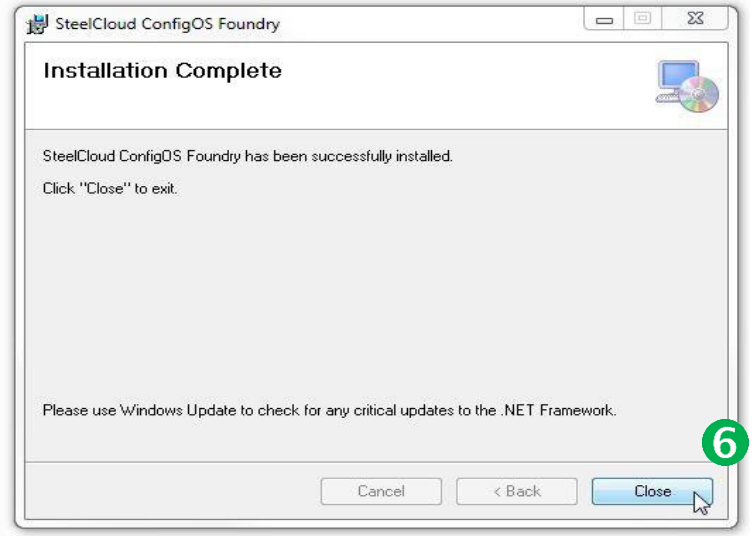
2 You can use the default program location, browse and/or create your own.

3 You can also install the Foundry for yourself or any of the users on this particular computer.

4 Click "***Next***" to go to the Foundry installation ready confirmation screen below.



5 Click "***Next***" to go to install the Foundry and you should see the "Installation Complete" screen below.



6 Click "***Close***" to go close the Foundry installation process.

E. Starting the ConfigOS Foundry

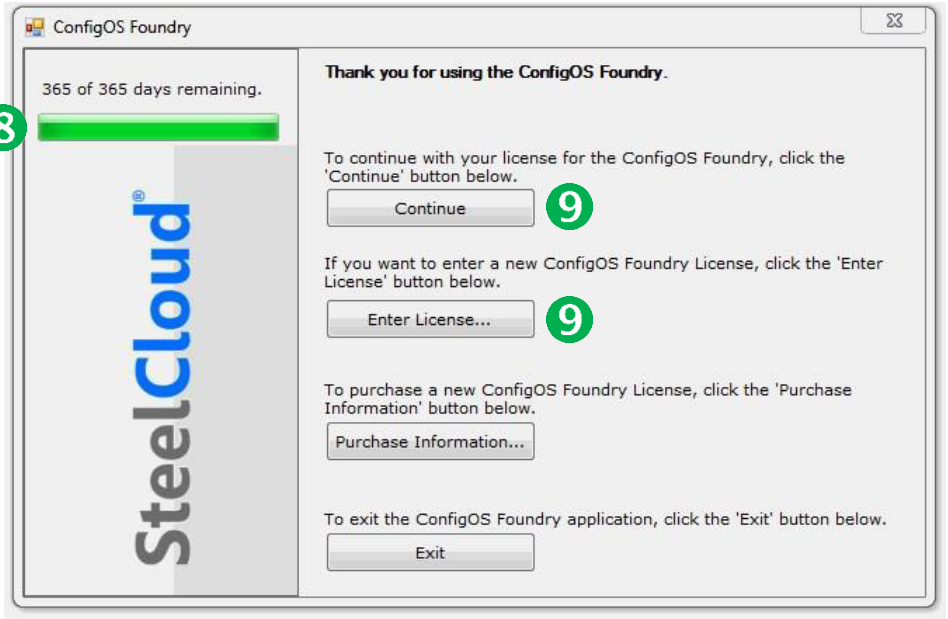
Go to "**START**" and "**Programs**" and select ConfigOS Foundry (below).

☑ ***Key Concept*** *– ConfigOS usage is based on a Product License Key. The Product License Key is an alphanumeric string that tells which features are licensed and for what period of time. The Product License Key is only requested the first time ConfigOS is run unless the product has a "timed" license such as a 10-day evaluation key.*

The first time that the ConfigOS Foundry is started you will be asked to enter a Product License Key. You will be presented with the screen below.

7 Browse for your Product License Key (which is a file with a "**. Lic**" extension) and select '***OK***.'

If a "timed" Product License Key has been entered, you will see the following screen each time you start ConfigOS.



8 The upper left corner displays the days left before your license expires.

9 The two primary options on this screen are to '***Continue***' to use the current key, or to '***Enter License***' to update ConfigOS with a new Product License Key.

Also, the first time that ConfigOS Foundry is run, you will have the opportunity to create a new pair of encryption keys (one for the Foundry and one for the ConfigOS Client) or to use a Foundry Key already created by another Foundry. You will be presented with the ConfigOS Key creation screen the first time (and only the first time) that you run the Foundry:

You have two options:

1. You can browse for an existing Foundry Key if you are adding this Foundry to an existing Foundry(s) and you want both/all to have the same Foundry Key. All Foundries installed with the same Foundry Key can produce/encrypt Signatures that can be utilized by the end point ConfigOS clients installed with the matching Client Key. If you select this option, the system will prompt you for the location of the Foundry Key that you want to use for the installation of this instance of the Foundry.

2. Or, you can create a new pair of keys (Foundry and Client) if this is the first Foundry instance that has been set up to service a given set of end point ConfigOS clients. If you select this option, the system will prompt you as to where you want to store the keys.

3. Select "**OK**" and you will see the following screen:

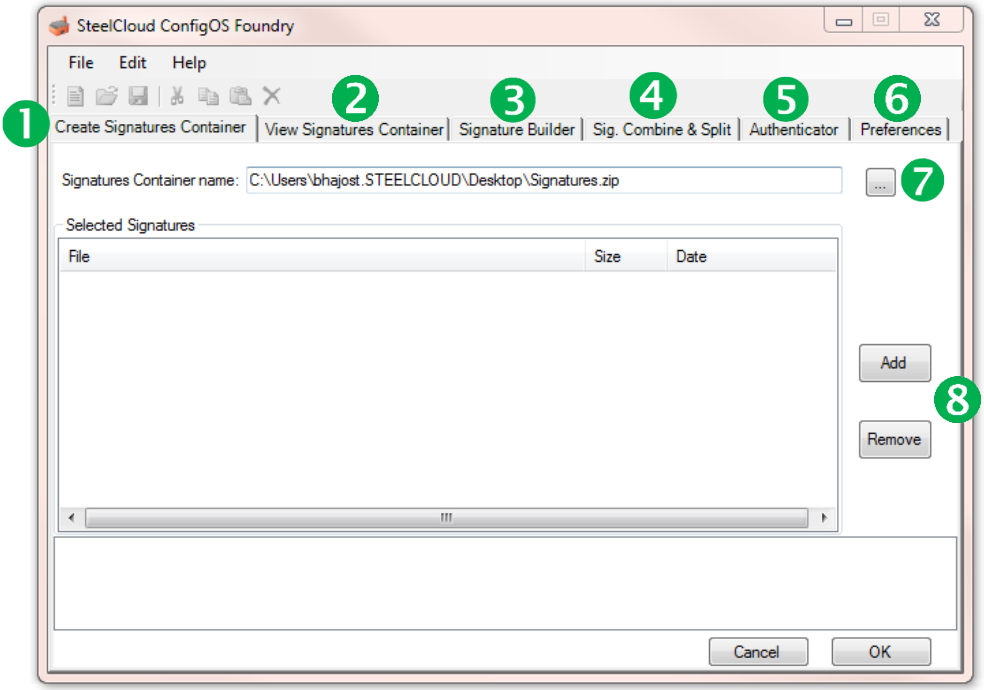
☑ ***Key Concept*** *– It is important to understand ConfigOS key generation and usage. The Foundry uses the FIPS-compliant random number generator within Microsoft Windows to generate a pair of 256-bit keys. The pair includes a Foundry Key and a Client Key. Both keys are encrypted so they cannot be read. The Foundry Key is used to set up one or more additional Foundries (all having the same key). The Client Key is the key that is used when installing the ConfigOS Clients. This keying mechanism is what ties one or more ConfigOS Clients to one or more ConfigOS Foundries. So, once*

a ConfigOS Client is installed with the Client Key generated by a Foundry, or set of Foundries using the same Foundry Key, it will only be able to decrypt/use Signatures that are created by that Foundry(s). The Foundry Key is different from the Client key because it was imperative that a user could not take a Client Key and use it to set up a new Foundry – thus bypassing the inherent Signature protections within ConfigOS.

☑ ***Key Concept*** *– Store these keys in a safe place. The Client Key will be used in the installation of all the ConfigOS Clients associated with this Foundry. The Foundry Key will be used to set up additional/back-up Foundries if you have licensed additional ConfigOS Foundries.*

F. Foundry Main Screen

ConfigOS Foundry has a very simple interface.



Functions provided on the Foundry main screen are as follows:

1. Create a new encrypted Signature Container by combining with one or more XML Policy Signature files with desired user documentation file(s). **NOTE:** Only XML Policy Signatures will be encrypted, user documents will not.

2. View the Policy and user files that are in an existing Signature Container.

3. **Signature Builder** – This is the Foundry facility that allows the user to tune/edit/extend existing signatures (or build new ones from scratch).

4. **Sig. Combine / Split** – This is the Foundry facility that allows the user to consolidate multiple individual XML policies into a single larger XML policy file (such as combining all of the individual Microsoft Office policy files into a single consolidated policy). This facility also allows the user to automatically "*split*" a larger policy into smaller parts to help accelerate policy testing in order to determine which policies need to be adjusted to allow an application environment to operate properly.

5. **Authenticator** – New with the 1.09 release of the Foundry, SteelCloud will begin publishing software and policy XML signatures in an encrypted package in order to further authenticate/protect our product support files. The Foundry Authenticator provides a facility to unpack/decrypt SteelCloud software and signature files.

6 **Preferences** – New with this release of the Foundry. This function allows the user to designate the location where the Signature log and User configurations will be stored.

7 Allows the user to create a user-defined name and location for a new Signature Container.

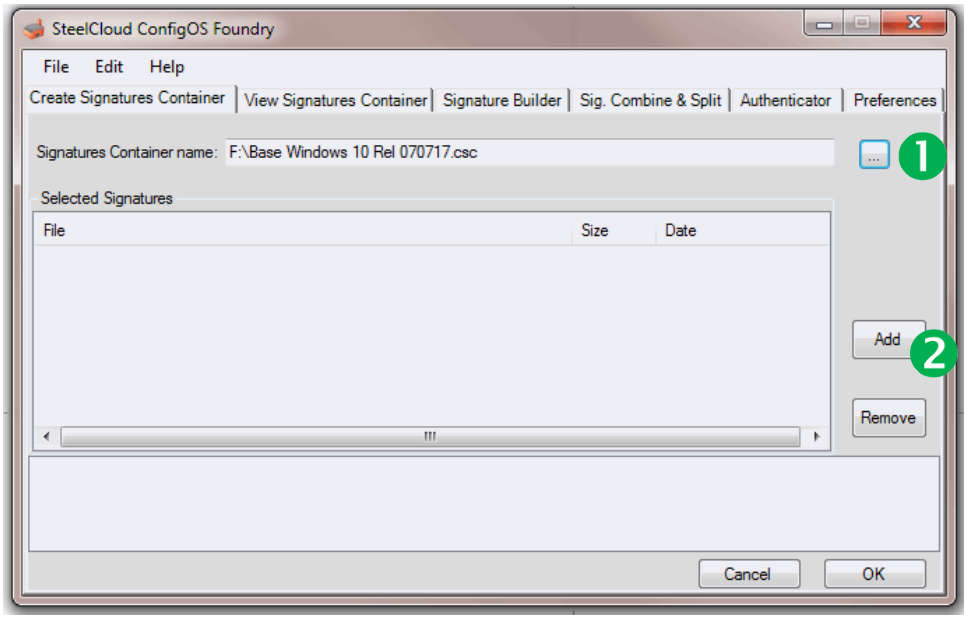
8 The Buttons to add and remove individual Signature and user files to/from a Signature Container.

G. Creating a New Signature Container

From the Main Foundry screen select the Create Signature Container tab.

The first thing we will do is to "**Name**" the Signature Container that we want to create and determine where we want to **Store** it. Select the "*Signature Container Name*" button below. 1

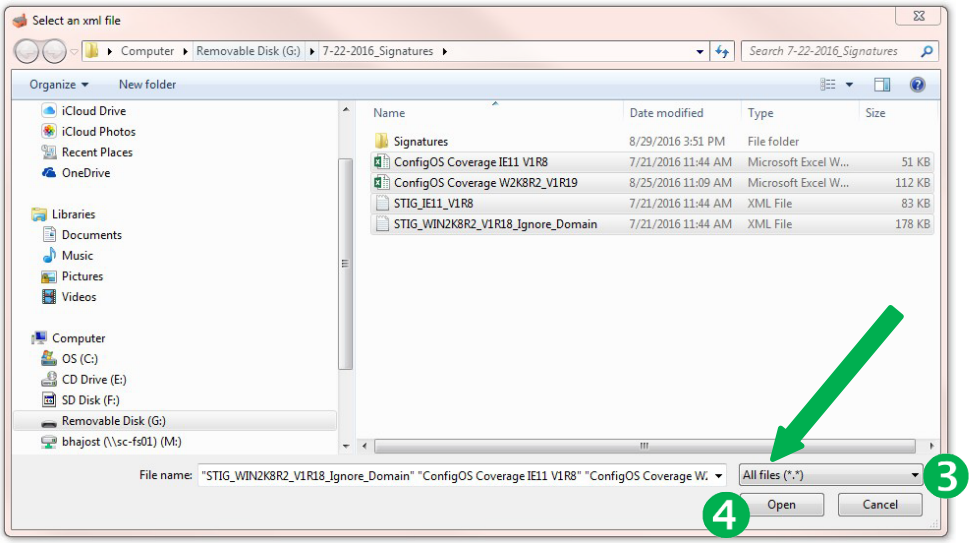
Locate the folder where it will be stored and a descriptive name for the signature container.



The next thing we will do is add the files that we want to include in the Signature Container using the "**Add**" and "**Remove**" selection buttons.

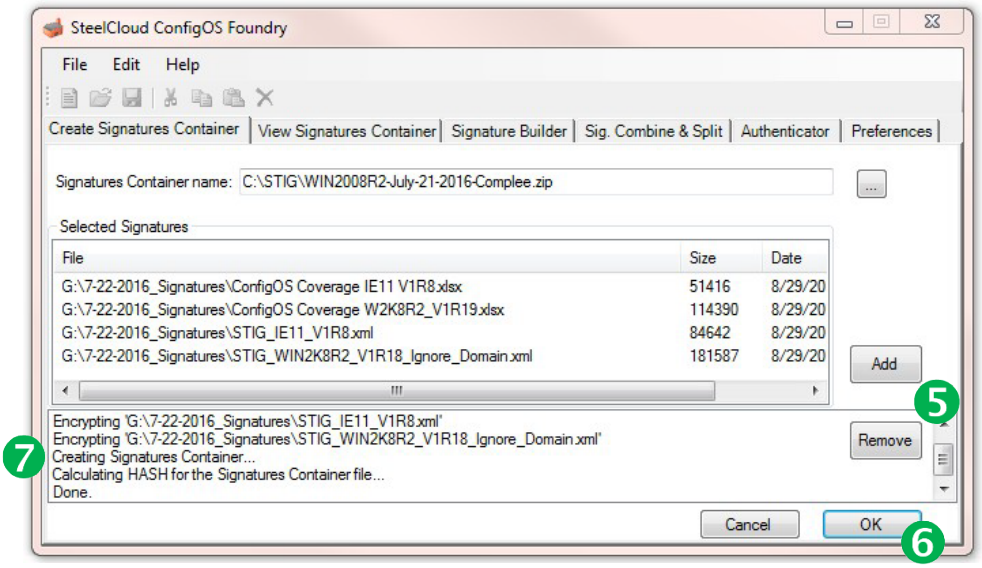
2 By selecting the "**Add**" button you will be able to search your file locations for the appropriate XML signatures and files that you determine that you want to include in this Signature Container. Below we have selected several Policy XML files along with some additional documentation that we want to include in this Signature Container.

3 **NOTE:** Make sure the "**File Type**" selector is set to "**All files**" if you want to include non-XML file types in your Signature Container.



In the above example, we have selected four files that we want to include in the Signature Container which we named on the previous screen. You will notice that these include a combination of both XML policy files (2008 R2 & IE 11) as well as user files (XLS).

4 "***Click***" on the "**Open**" button and you will see those files populated to the Foundry Signature Container Screen below.



5 You can add or delete individual files to the Signature Container using the "**Add**" and "**Remove**" buttons.

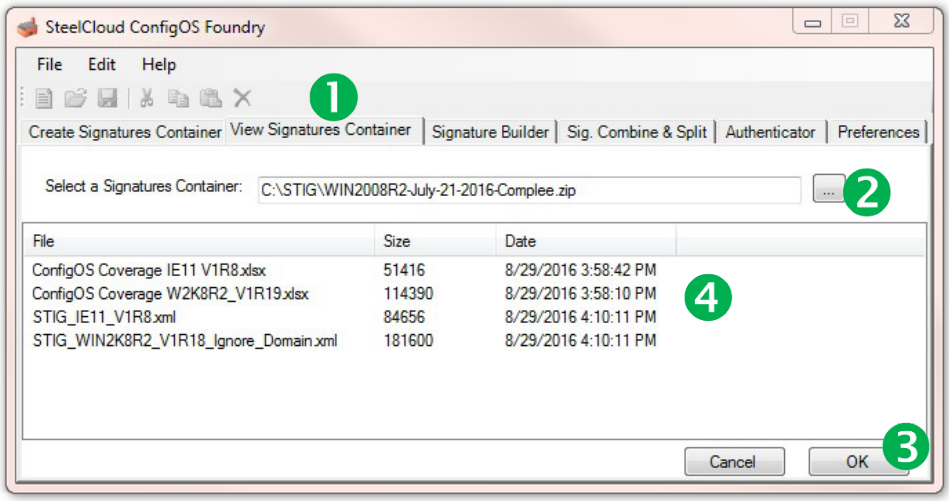
6 If everything is as you want it, select the "***OK***" button and the Foundry will create the container *(encrypt, hash & zip)*. The dialogue at the bottom gives you the status of what the functions Foundry performed. 7

☑ ***Key Concept*** *– ConfigOS creates a log file in "**csv**" format that contains pertinent information for every encrypted Signature Container that is created for a given Foundry. This file is stored in the location specified in the "**Preferences**" tab. It is important that the user selects a discrete location for each Foundry in use. The contents of this log file are protected by a tamper-resistant mechanism. Manual edited of this log file will be recognized and indicated by ConfigOS when a new log entry is recorded.*

H. View Signature Container

Let's look at the Signature Container that we just created. On the Main Screen select the "**View Signature Container**" tab. 1

2 Now, select the location/name of the Signature Container that we just created and select "**OK**." 3



4 You will see the individual files contained in our Signature container. There are two Policy XML files and two XLSX support documentation files.

I. Miscellaneous

Under the "**Help**" menu you will find two important functions (below).

The "**Key**" selection will give you the file name of the key that is being used to encrypt the XML files. This is useful in ensuring that ConfigOS clients are using the same key. The ConfigOS Client manager will have the same key with the designation "ClientKey."

The "**About**" selection give you the ConfigOS Foundry Version information along with the License expiration date.

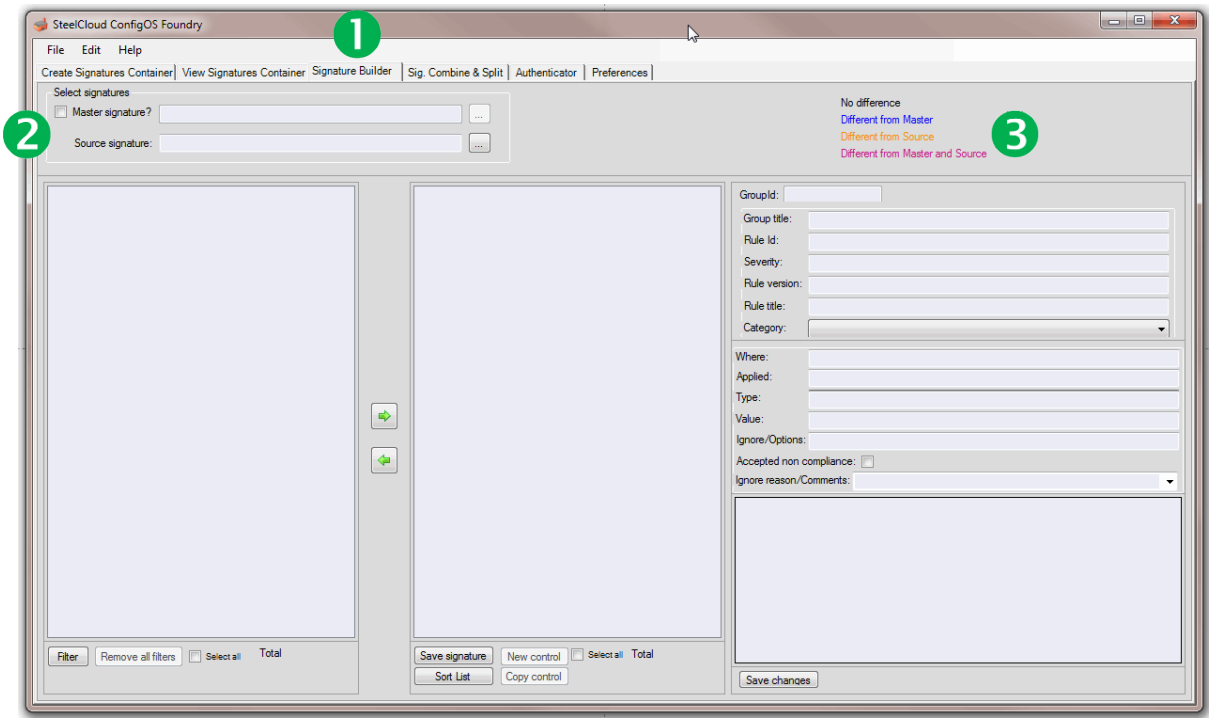
J. The Signature Builder

The Signature Builder ("Builder") an easy to use, flexible tool for creating, cloning, modifying, and editing ConfigOS Signatures without the need to edit the underlying XML. The Builder works with clear text XML exclusively. The new XML Signature created by the Builder, is processed through the standard Foundry packaging/encryption process described earlier in this document.

The Builder's primary use cases are as follows:

- Take a subset of an existing signature to make a new signature. This is useful in hardening a system around an application by implementing policy (and reversing policy) using a small subset of the policies of a complete Signature.
- Edit the values in an existing Signature and creating a new Signature.
- Adding policies to an existing Signature.
- Creating a new Signature from scratch. This facility is appropriate for creating both small targeted Signatures as well as large Signatures with 100s of controls.

To access the Foundry Builder, select the "**Signature Builder**" tab. 1



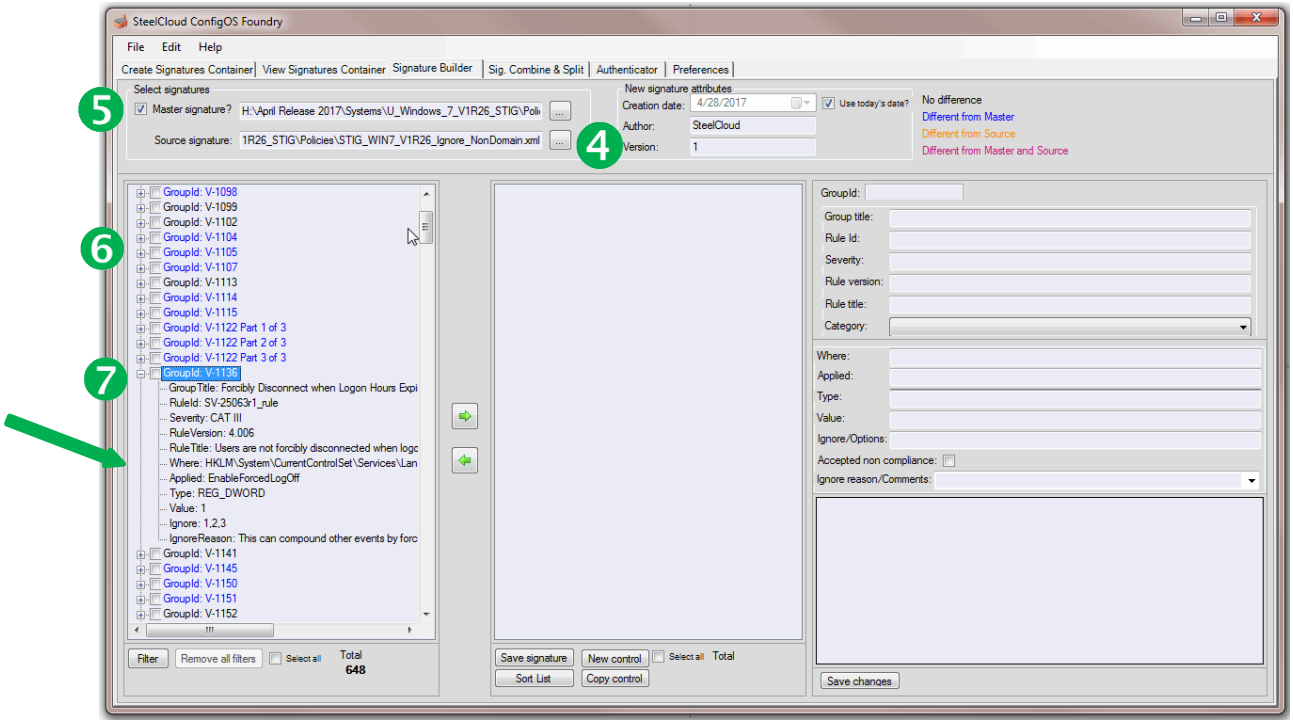
2 The Builder allows the user to select a Master and Source Signature. The Master Signature is only used for reference and validation. The Source Signature is the one used as the basis for creating the new Signature.

☑ ***Key Concept*** *– Consider the "Master" Signature to be the enterprise standard signature, such as the STIG benchmark Signature. By validating against a Master Signature, as Signatures are modified/created, the user can always tell the waivers and exceptions that exist in the new Signature as compared to the "Master" Signature standard. The Master/Source Signature set-up will also allow you to compare the differences in two signatures (i.e. this quarters vs. last quarter's policy)*

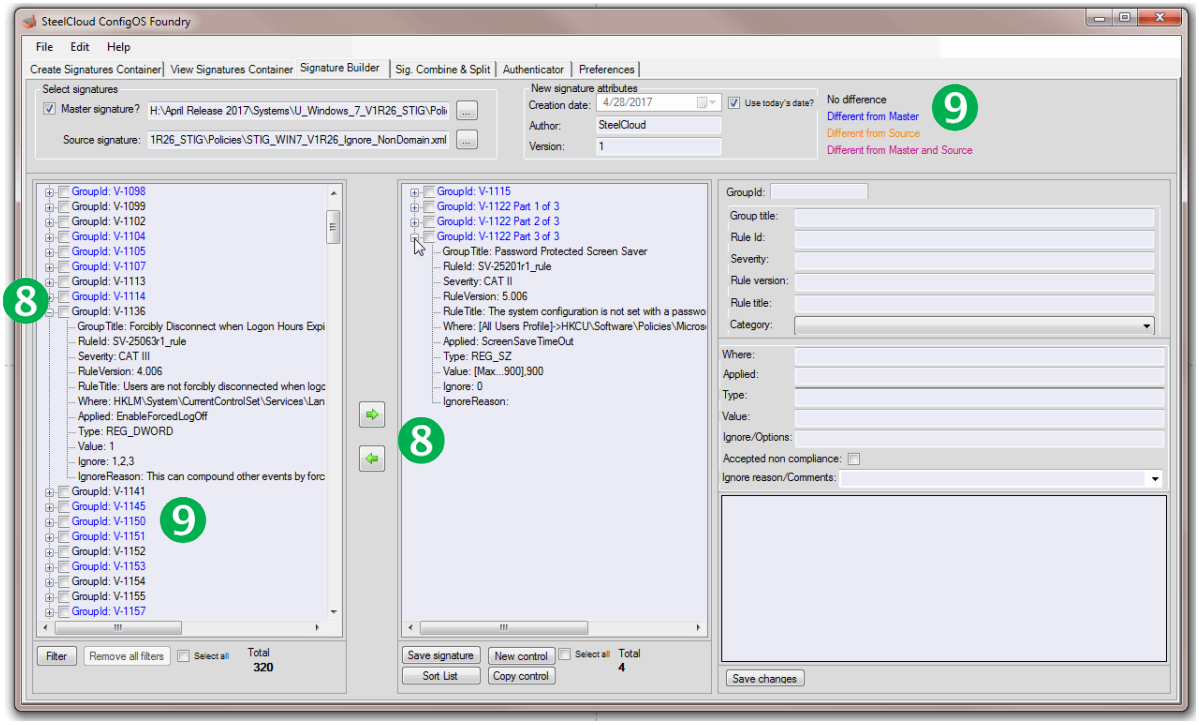
3 As the user works with creating/modifying a Signature, they can see that the resultant Signature differs from the Master, the Source, or both, by the color key in the upper right side of the Builder screen.

4 In the Source Signature entry line, click on the button to the right and select the Source Signature. The Source Signature is the working Signature from which you will use to "clone" to create a new signature, while the Master Signature is used only for validation purposes.

5 To utilize an optional Master Signature, click on the selection box at the left of the "Master signature" entry line. Then click on the button at the right of the Master signature line to locate the Signature that is used as the standard for your Signature build process. In the example below we have selected the "Master STIG" Signature.



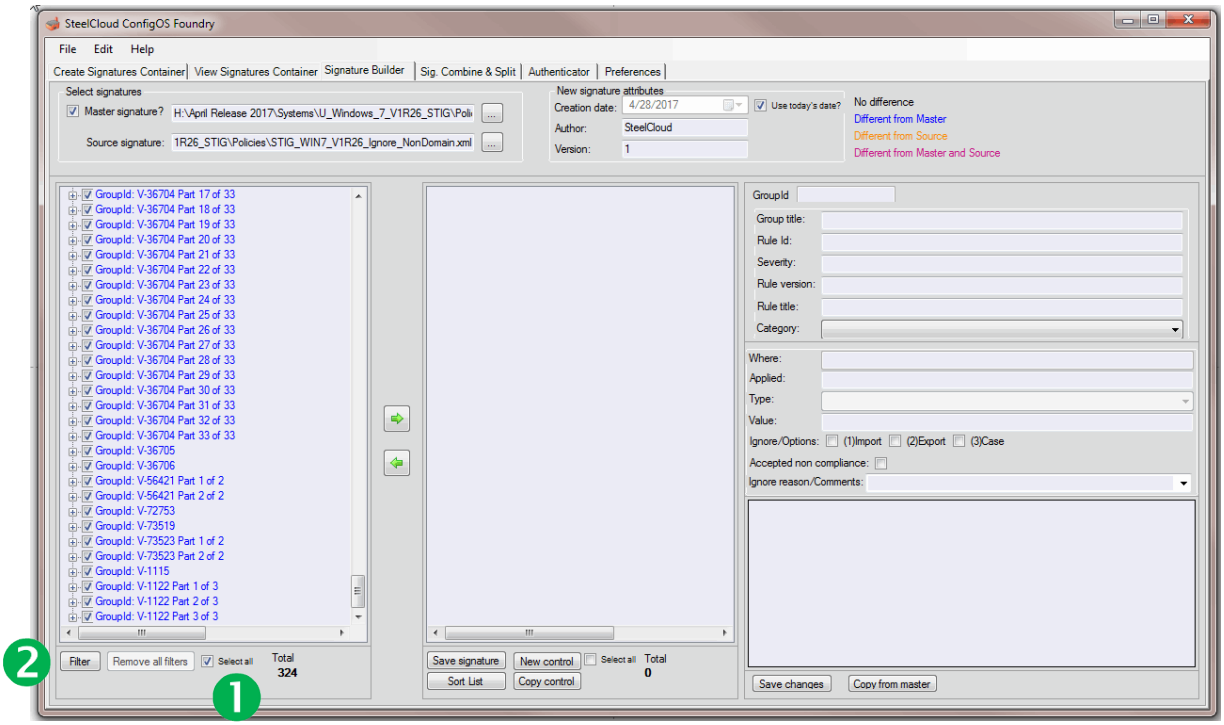
6 The contents of the Source Signature are displayed in the left Signature box. More information is available on each control by clicking on the "**+**" next to the control. Selecting the "**-**"will collapse the control description. 7



Individual controls are selected by "checking" the boxes next to the controls. Once one or more of the controls are selected in either the left or right Signature box, the "Arrow" keys can be used to move the controls between the left "Source" Signature box and the right "New" Signature box. 8

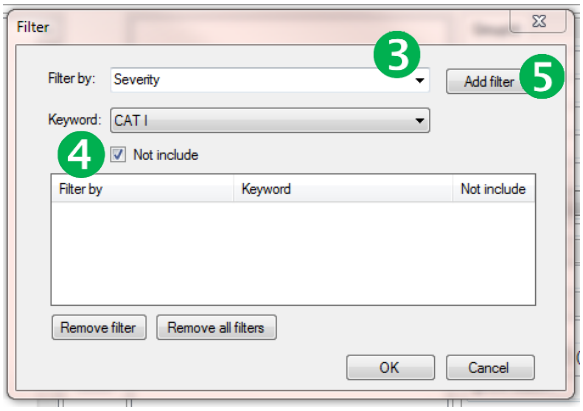
9 A number of the Source Signatures Controls (*in Blue*) are different that our Master Signature. The color-keyed description in upper right portion of the screen indicates the various differences between Master (*Blue*), Source (*Orange*), or both Master and Source (*Red*) Signatures.

☑ ***Key Concept*** – *The Builder has two ways to make new Signatures fast and easy. The first is the "**Select all**" checkbox which will "check" all of the controls in the Source Signature Box (left) for a mass move to the New Signature Box (right). The second is "Filtering" that allows the user to select a sub-set(s) of the Source Signature controls by either including or excluding specific control information, and then moving that subset(s) of controls into the New Signature Box (right).*



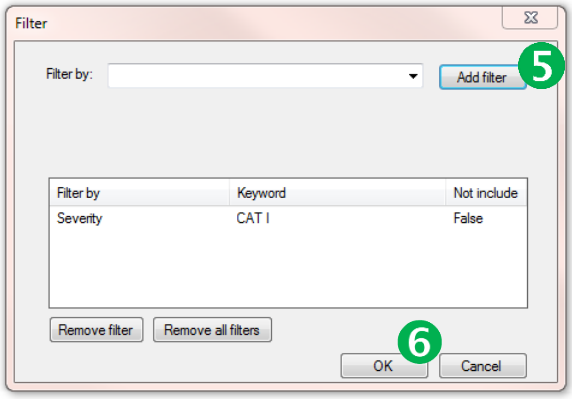
1 At the bottom of the left part of the screen is the "Select all" checkbox that will select all of the items in the left Source Signature Selection Box.

2 The Source Signature can also be "filtered" using the selection box at the bottom of the Source Filter section. When the "Filer" button is selected, the following dialogue is presented to the user.

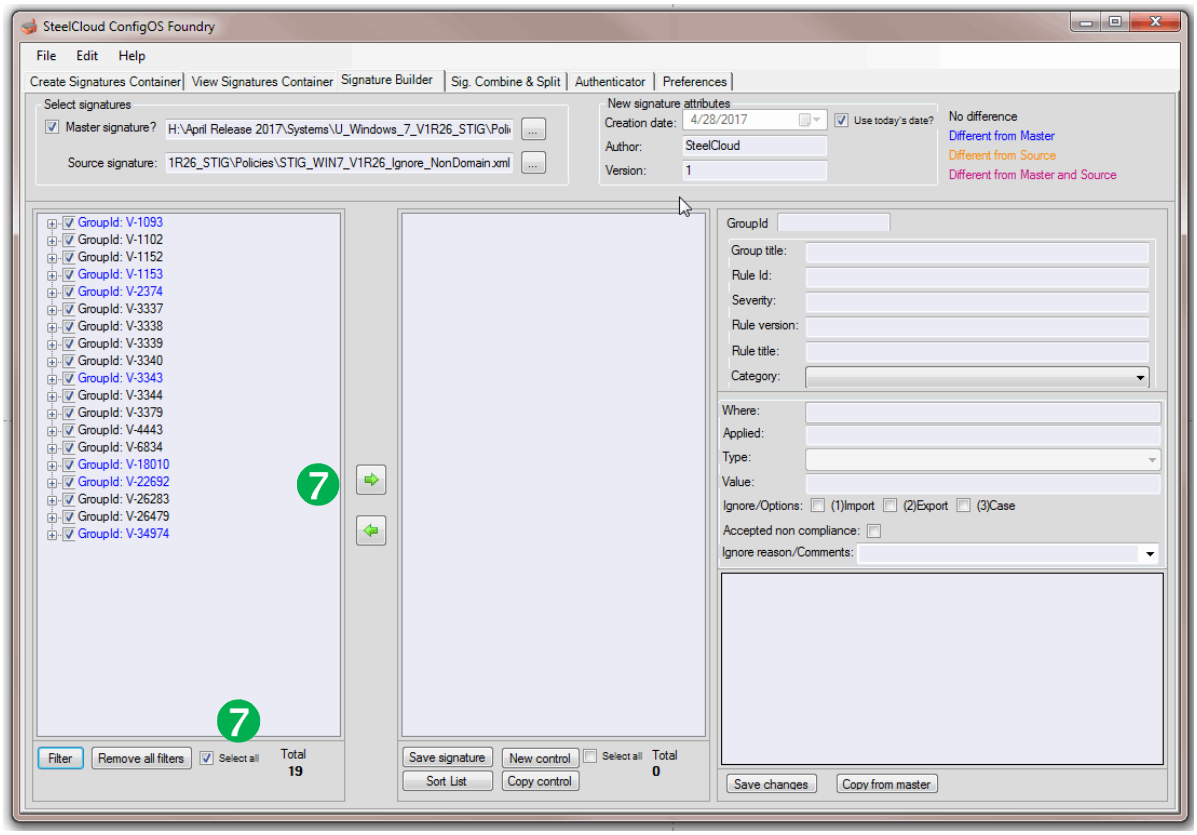


3 By selecting the "Filter by" down arrow the Builder presents the various options for filtering. Let's choose "Severity" and the keyword "CAT I." If we want to build a Signature including all of the controls except, CAT Is, we would select "CAT I" and check the "Not include" box. 4

5 Select the "Add filter" button to add the filter to the list. The user can continue to add additional filters the filter list to isolate only those controls needed for our new signature.

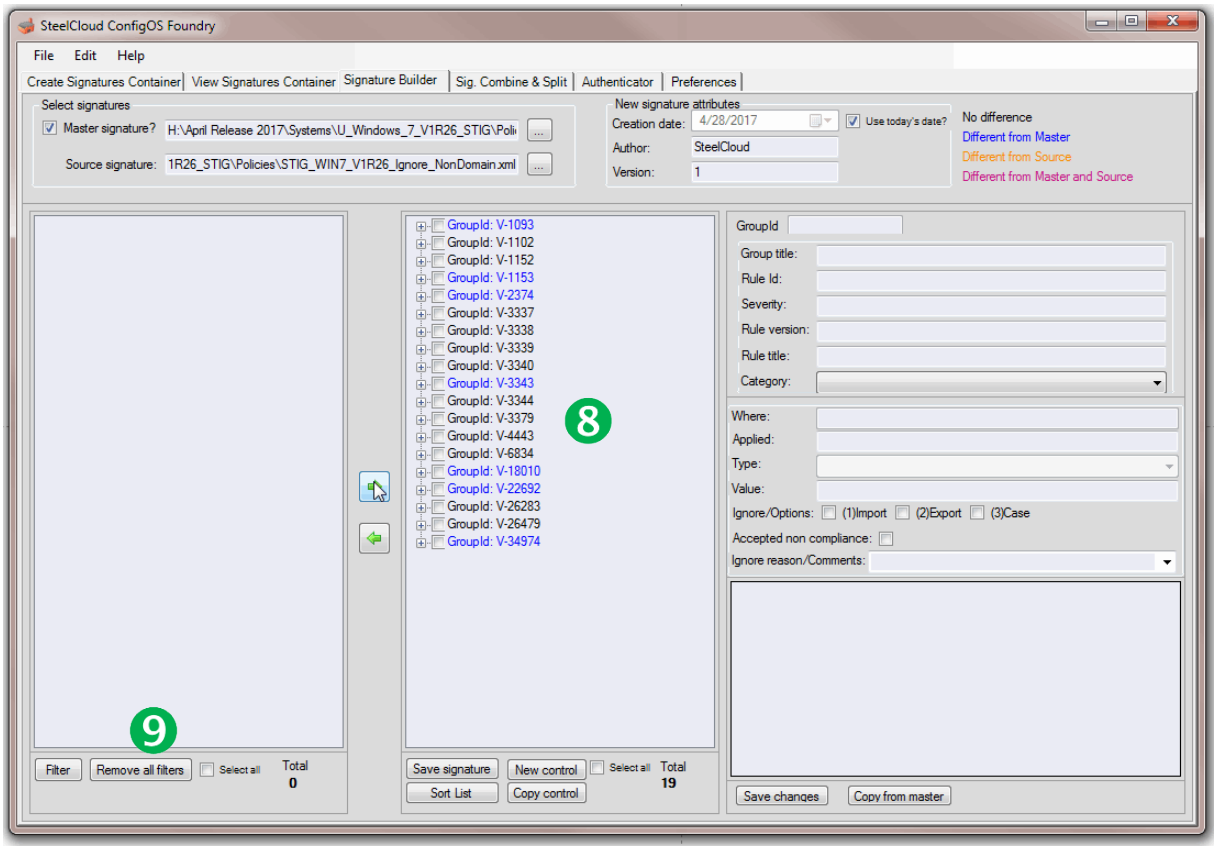


6 To apply the filter(s) select "OK" and the controls that match the filter(s) will appear on the left section of the builder.

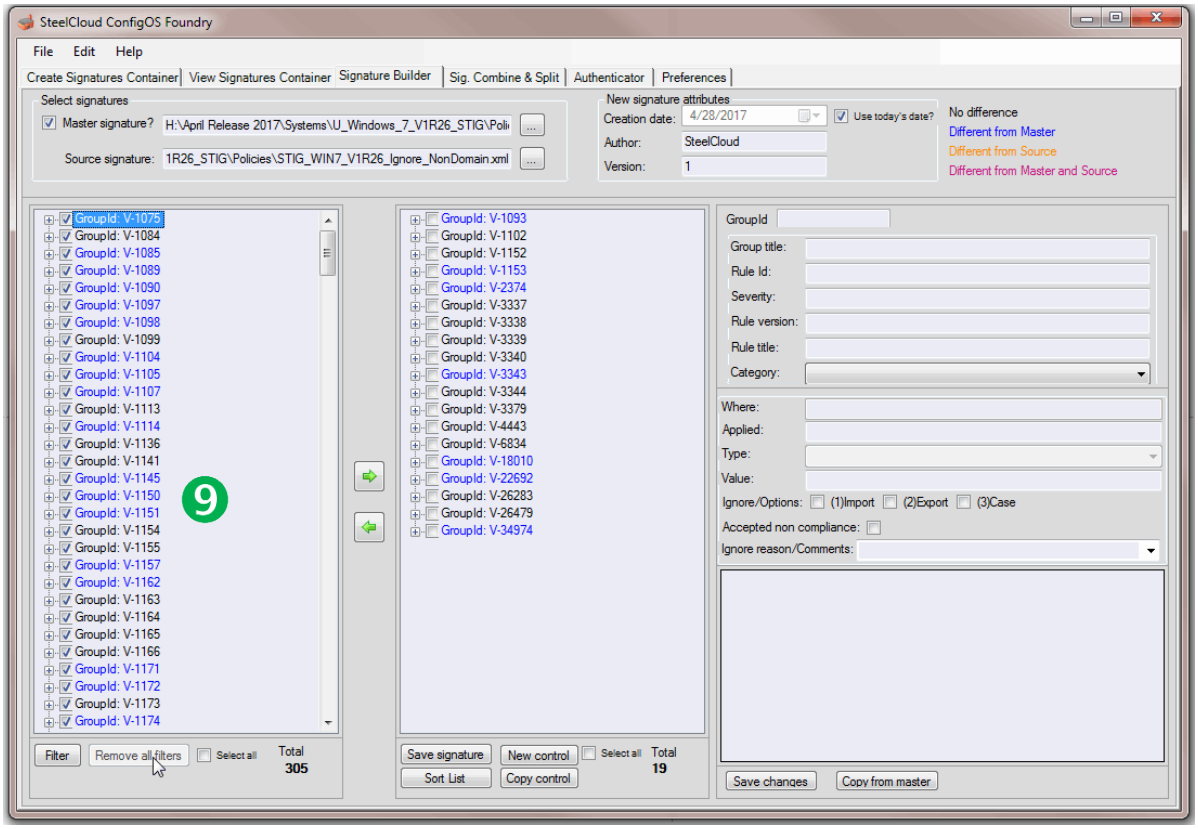


☑ ***Key Concept*** *– For both Windows and Linux Signatures, selecting "Filter by" "All" will allow the entry of an ad hoc text string. In both Windows and Linux, when selecting a "Filter by" category of "Severity" the user will be presented with "CAT I," "CAT II," or "CAT III." With most of the other "Filter by" types in Windows the user will be presented with a list of choices. Linux Signatures only provide a list of choices for "Severity."*

7 We would the “check” “Select all” and select the “Right Arrow” button and we would see all of the controls that met our filter criteria have be moved to the New Signature Pane (*center*) as seen below. 8



By selecting the “**Remove all filter**” button all of the remaining control items that were not filtered will reappear on the left Source Signature Pane.



☑ ***Key Concept*** *– With the non-filtered controls is the Source Signature Box, the user can re-filter the remaining controls and/or individually select controls (check the box to the left of the controls) and move/add them to the controls in the center new signature pane.*

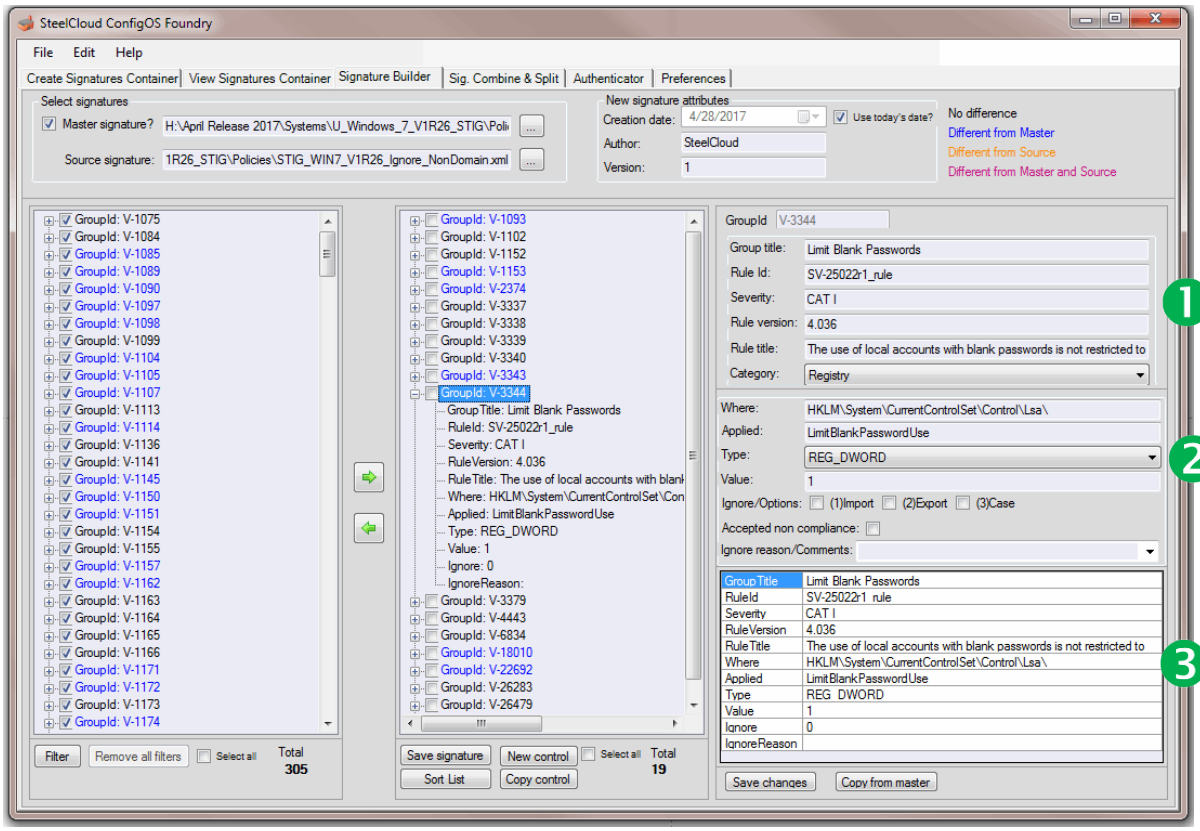
☑ ***Key Concept*** *–* ***Sort List*** *– Many times, especially for Linux, the order in which the controls are processed is very important to get the desired results, so the sorting function is available for Windows only. All of SteelCloud's published signatures are ordered properly. But, as a client adds new controls, there may be the requirement that the control's location in the processing stream be adjusted. The Builder gives the user the ability to reorder the controls in the center pane simply by dragging an individual control to a new location in the list (both up and down). This capability will allow you to ensure that the order of the controls is properly maintained to provide the desired results.*

☑ ***Key Concept*** *– Besides determining which controls to include and which controls to exclude from a Signature, the user can edit the actual control values in the XML Signature through this same Builder interface.*

Signature Editing: At this point in the New Signature creation process we have not yet saved the New Signature. Let's take a further look at the right part of the Builder screen.

There are three boxes on the right side of the builder screen. The control we have selected is identified at the top of these three boxes.

1. The top box is static information about the control.
2. The metadata in the second box changes based on "Category." Typically, controls will be edited in the second box.
3. The third box is a very important feature of the Builder. The third box displays the control information form the Master Signature that was entered when we started using the builder. As a user may edit a Signature, this Box allows the user to monitor how their changes are different from the Master Signature.



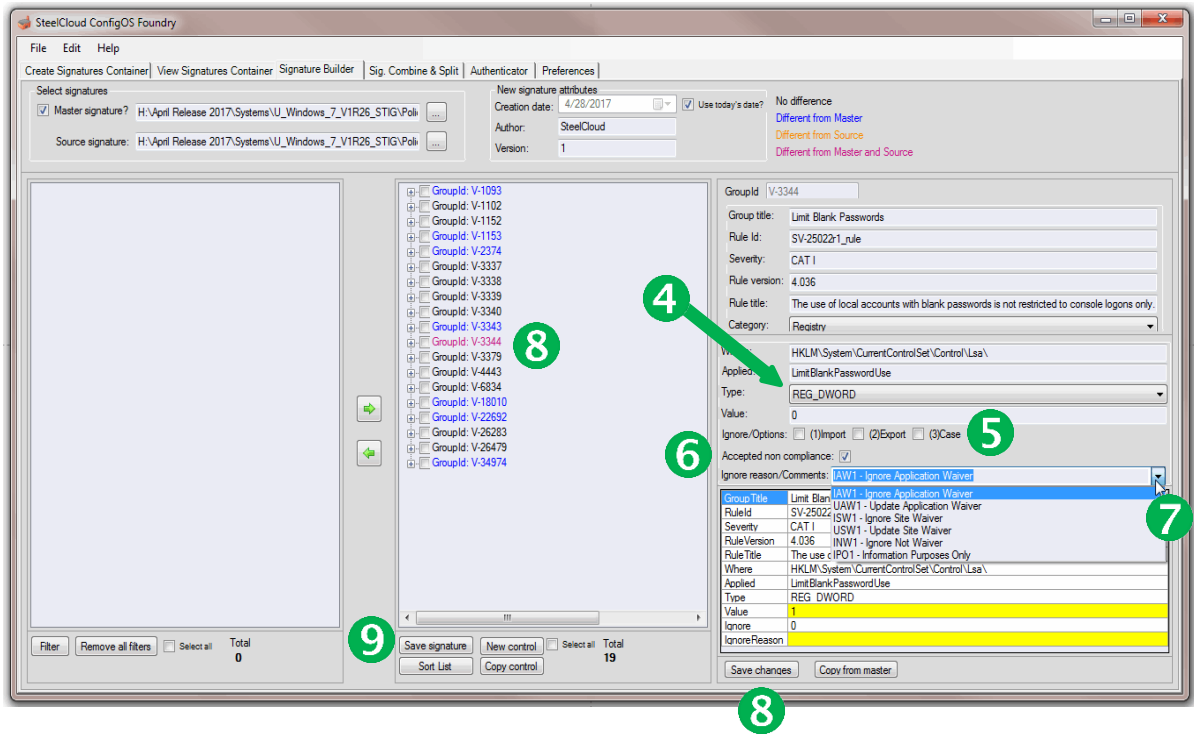
Here we have selected control "**V-3344**." The control name is indicated at the top of the right side of the screen along with the specifics of the control in the first two boxes.

We also see that the value is "***1***"- this means that the Signature will not allow "Blank Passwords." For various controls, ConfigOS will support ranges so value might be represented as *"**[1…3],3**"* which tells ConfigOS that the control can be between "**1**" and "**3**" inclusive with a default value of "**3**" which will be used if a system is out of compliance.

☑ ***Key Concept*** *– One of the most important features of ConfigOS is that it Compares and Remediates based on a "range" provided in the Signature (the DISA STIG in the case above). Therefore, ConfigOS will not show mismatches (deficiencies) and it will not*

Remediate (update) controls as long as they are within the range of the Signature. This allows a Signature to be used on a wide range of sites while reducing false negatives and unnecessary updates. If you prefer to Compare/Remediate to exact controls values, simple edit the controls for the values that you want.

4 Let's assume that our legacy application environment requires that we alter the value of control **V-3344** to allow for blank passwords. We simply change the *"**1**"* value to a "***0***" which is outside the STIG range, but required for the application to operate properly.



5 The user has the option to "*Ignore*" for ***Import*** *(Remediation)* and/or Export simply by "checking" the appropriate box. The user can also ignore case.

6 The "***Accepted non compliance***" checkbox is used to indicate that the change in this control has be accepted (waiver). If this box is checked for a control, it will be color-coded on the ConfigOS compliance reports indicated the waiver acceptance.

7 We could also provide an explanation of why we changed this control in the "***Ignore reason/Comments***" field. The "***Ignore reason/Comments***" field is a 1000-character field that can be used to describe why we altered and/or ignored a control. See the "***Preferences***" description for a further explanation of standardizing this field.

8 When the editing on a control is complete the user would click the "**Save changes**" button. After we have changed the value of the **V-3344** control information, this change is highlighted in the Master Signature box at the bottom right of the screen and the control is highlighted in red on the center pane as being "*Different from the Master and the Source"* Signature.

☑ ***Key Concept*** *– Foundry automatically validates several items when editing Signatures in order to catch a range of user errors. These include common XML syntax, Windows Registry Keys, and commonly used Linux command line entries.*

☑ ***Key Concept*** *– "Ignore" is a powerful feature in the ConfigOS Signature creation and remediation process. The user has the opportunity to ignore Import, Export, and Case. Ignoring Import allows a Signature to show differences, but will not update/remediate the target system. This is very useful around account controls where ConfigOS can determine that the set-up is wrong, but it does not know the specific customer account information to update the target system. Ignore Export is a more specialized function for using a Master Signature for exporting Source System information. When "Ignore Export" is selected, the export process will "plug/override" the values in the Signature rather than what is in the Source System. And, Ignore Case simply will not show differences or remediate systems based on the "case" differences between the Signature and target system text. The user can enter an explanation for the waiver/ignore in the box provided. The "**Ignore reason**" allows the user to document why changes to the policy were made. The entry in this field will be shown on the scan/compare screens as well as ConfigOS compliance reports.*

✋ ***Caution*** *– It is recommended that the customer does not edit individual IIS signature controls. However, there are no issues with "ignoring" or removing individual controls. For additional support, please contact SteelCloud.*

Save the New Signature – Finalization of a new signature is a simple two-step process.

8 1. First, when the user is done editing the new Signature, they **must** click the "**Save Changes**" button and the changes will be saved in a work space.

9 2. Next the user would click the "**Save Signature**" button which will bring up a standard dialogue were the user will select a name and a location for the Signature (file). It is preferable that the name of the Signature be as useful and descriptive as possible.

☑ ***Key Concept*** *– Keep in mind that the control information, as edited or ignored, and the ignore reason will become part of a secure, encrypted, tamper-proof Signature after this file goes through the standard Foundry process.*

☑ ***Key Concept*** *– If the name given to the new edited Signature already exists in the same folder to be saved, the Foundry will warn the user. If the user selects "**Yes**" to proceed with the over-write, the Foundry will rename the original Signature with a "**bak**" extension to keep from inadvertently writing over a valuable Signature. To reuse the original Signature, the user would simply rename it with an "**xml**" extension.*

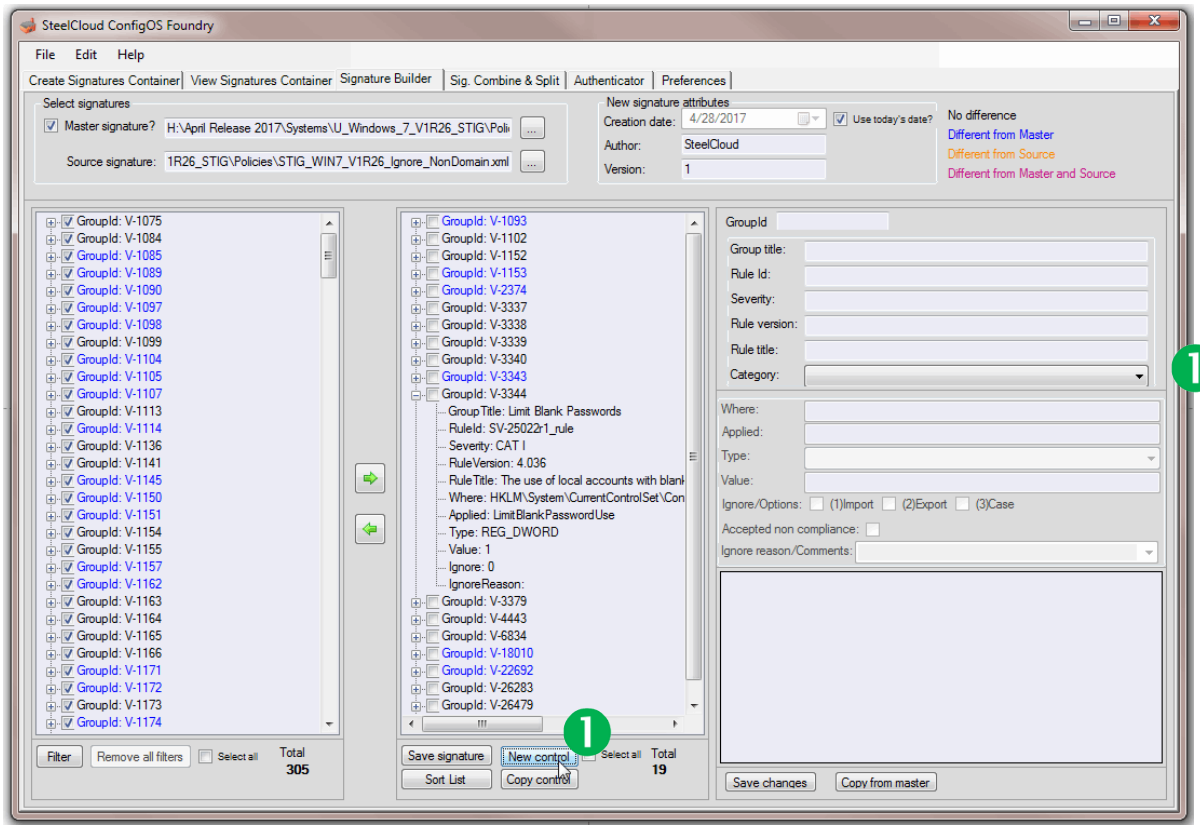
Ignore Reason - "***Ignore reason***" is used by ConfigOS to display the reason that a particular control is ignored and/or why the control was edited/changed. This field lets the user document exactly why the changes were made. ***Ignore reason*** is also printed on certain reports and logs. ***Ignore reason*** is searchable for those use cases where you might want to select all controls that have been changed or ignored. ***Ignore reason*** is free-form and its use is optional. At SteelCloud, we use the following ***Ignore reason*** nomenclature:

- ***IAW1****- (Ignore Application Waiver) = This designation is used where a control is* ***ignored*** *and a waiver is required for an application to operate properly. This information would typically only be entered by the user.*
- ***UAW1****- (Update Application Waiver) = This designation is used where a control is* ***updated*** *outside of the STIG range and a waiver is required for an application to operate properly. This information would typically only be entered by the user. (This is used in the example above).*
- ***ISW1*** *(Ignore Site Waiver) = This designation is used where a control is* ***ignored*** *and a waiver is required based on the requirements of a site rather than an application. This information would typically only be entered by the user.*
- ***USW1*** *- (Update Site Waiver) = This designation is used where a control is* ***updated*** *outside of the STIG range and a waiver is required based on the requirements of a site rather than an application. This information would typically only be entered by the user.*
- ***INW1*** *- (Ignore Not Waiver) =These ignores are the safeguards built into the ConfigOS Signatures that flag STIG deficiencies, but to not attempt to update controls without additional information. Manual processing is required, such as which is the proper account to go the proper group. SteelCloud uses this designation for those controls that we can validate, but not remediate.*
- ***IPO1*** *- (Information Purposes Only) = This is information useful to the customer such as alternative passing values, information specific to specific sites, and other information that does not involve the need for a waiver. SteelCloud uses this designation primarily in our Linux signatures.*

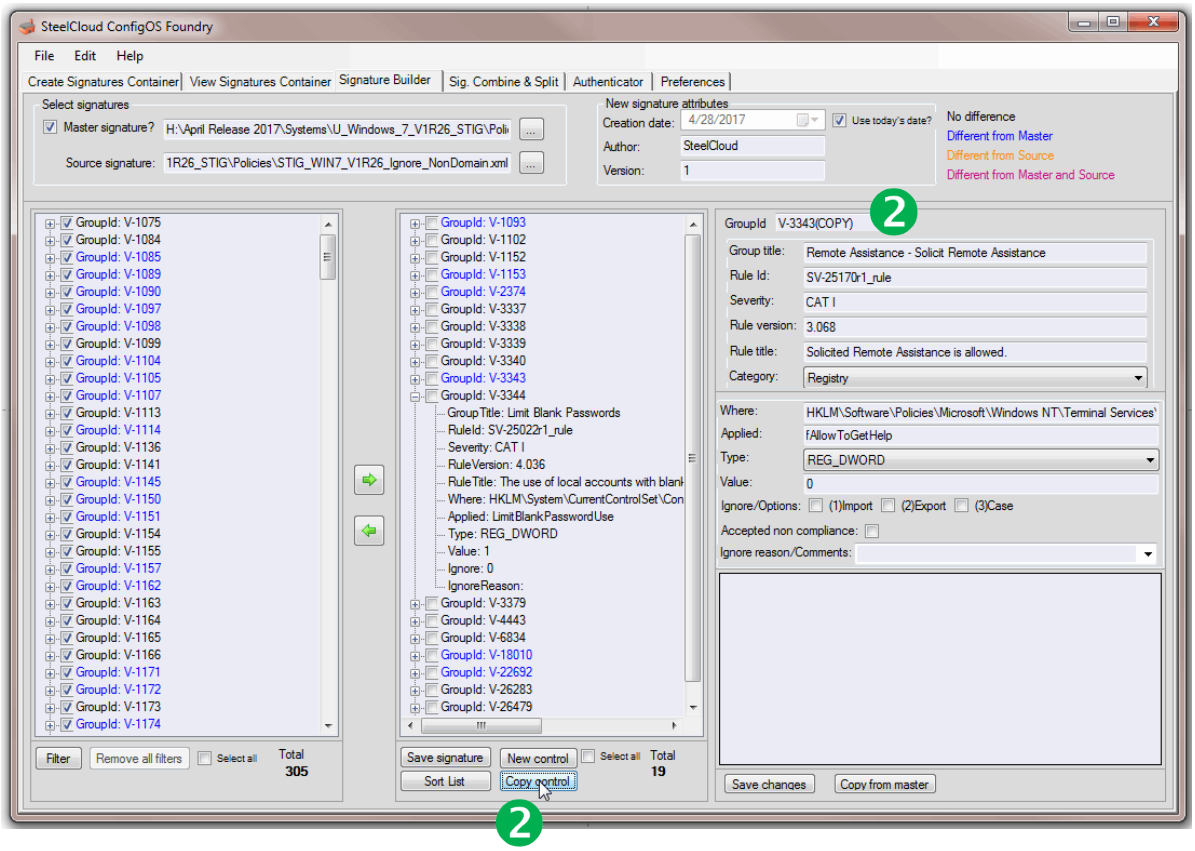
Setting Default Ignore Reason Codes – Default Ignore Reasons can be set up by editing the "***User Configuration File***" accessible at the location specified on the "***Preferences Tab***."

New control & Copy control Functions – The "**New control**" and "**Copy control**" functions allow a user to quickly add and extend Signature Controls.

1. The "**New control**" function allows the user to add a Control (GroupId) into a Signature for which the user would edit all of the Control information. This is useful when no existing Control can be cloned and edited. By selecting "**New control**," all of the fields to the right of the screen are "blanked out" and ready for the user to enter the new control information.



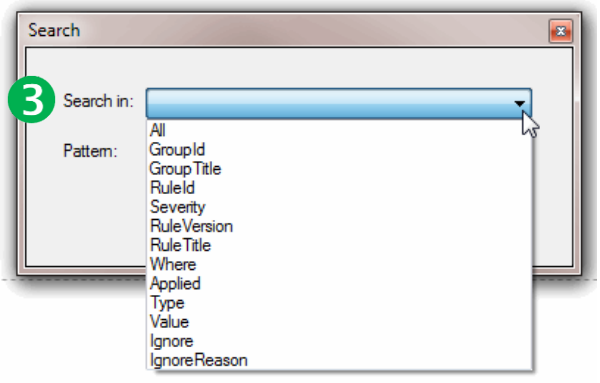
2. The "**Copy control**" function allows the user to select and copy (clone) an existing Control that the user would then modify to create a new Control. All of the information from the control is populated in the panes to the right and "***(COPY)***" is appended to the **Group ID**. All of the control information can now be modified.



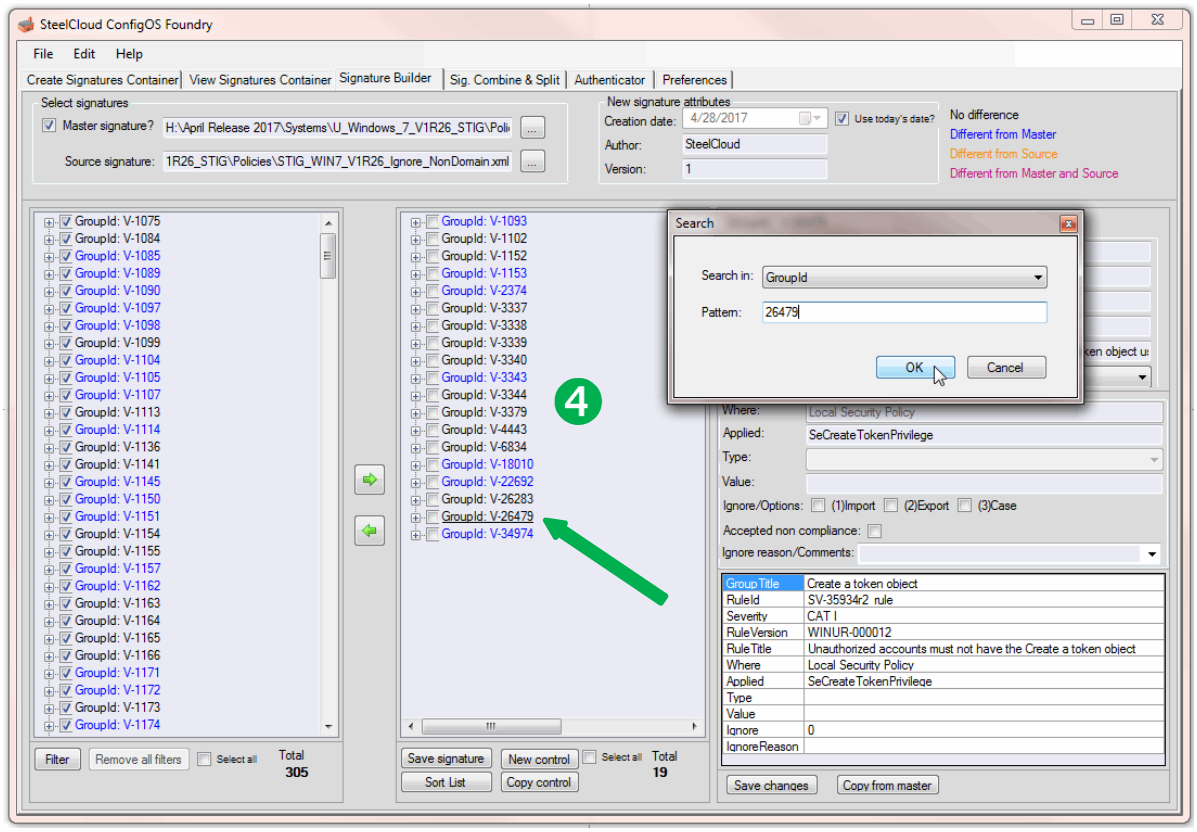
With a little practice, the Foundry Signature Builder provides a productive facility to build and modify Signatures while providing visual confirmation of the results.

☑ ***Special "FIND" Functionality*** *– The Signature Builder provides a special "**FIND**" function for data contained on the center panel. It works somewhat like the "Filter" function on the left panel and allows the user to quickly locate a control (or controls) that match a text search. Users have the same metatag functionality to be able to search only within a specific tag such as Severity. See the example below where a specific V-ID is located. The **FIND** function is invoked by "**Ctrl-f**."*

3 After invoking the **FIND** function, the pop-up will appear. Select the desired "**Search in**" meta tag



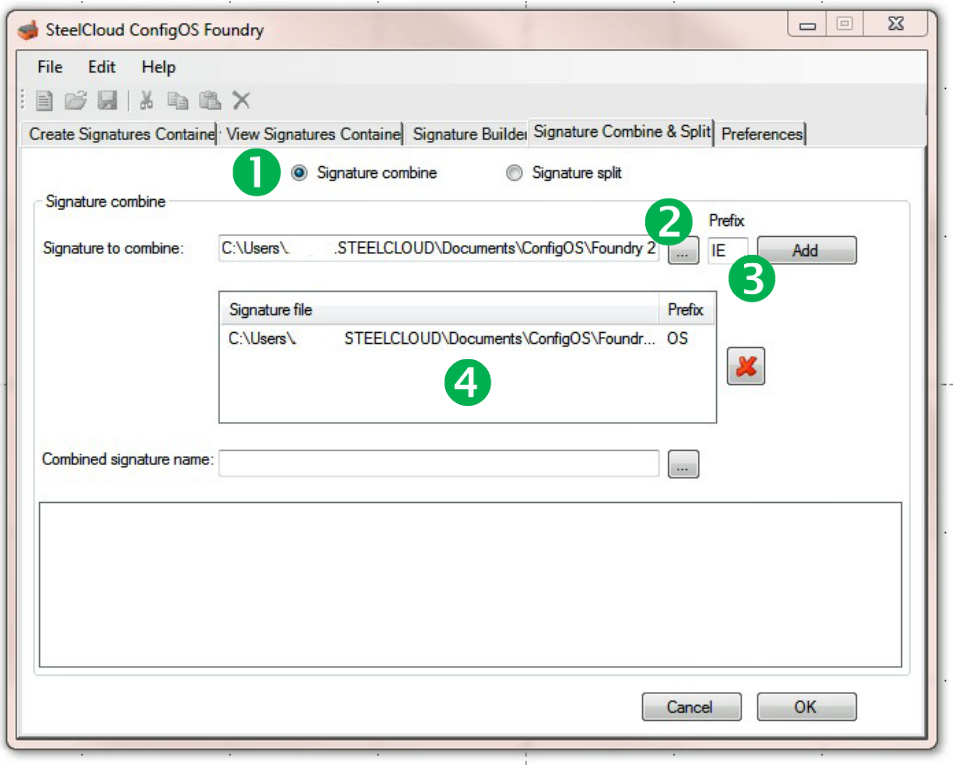
Next, enter the search information in the "**GroupID**" field, (such as "**26479**") and selecting "**OK**." The control(s) that match the criteria will be highlighted. 4



K. Signature Combine & Split

The Signature Combine & Split ("SC&S") is available as a "**Tab**" in the Foundry version of the ConfigOS Foundry product. The SC&S is a simple to use tool that has two functions. First, the "**Signature combine**" function allows the user to take multiple individual XML policy files and combine them into a new, consolidated policy file. Additionally, the "**Signature split**" function will automatically break a single policy file into two to five separate/equal policy files. These smaller policy files are useful in the process of determining what controls will have to be adjusted (waivered) to allow an application to operate.

☑ ***Key Concept*** *– The use case for combining signatures is fairly straight forward. Certain benchmarks, such as the DISA STIG, publish each component into a separate benchmark document. This would include components such as each application in the MS Office Suite, IE, .NET, etc. Therefore, SteelCloud signatures are published to line up, one-for-one, with the DISA documents. For convenience, a user might want to combine two or more components into a single signature to simplify the scanning, remediation, and reporting process. The ConfigOS Signature Combine feature allows the user to safely and simply accomplish this task.*



Signature Combine is a fairly simple to use facility.

1. Ensure that the "**Signature combine**" button is selected.
2. Select the clear text XML signatures that you want to combine by selecting the "**File**" button and locating the appropriate clear text XML signature. NOTE: Select the

individual clear text XML signatures in the order in which you want them combined in the final consolidated signature.

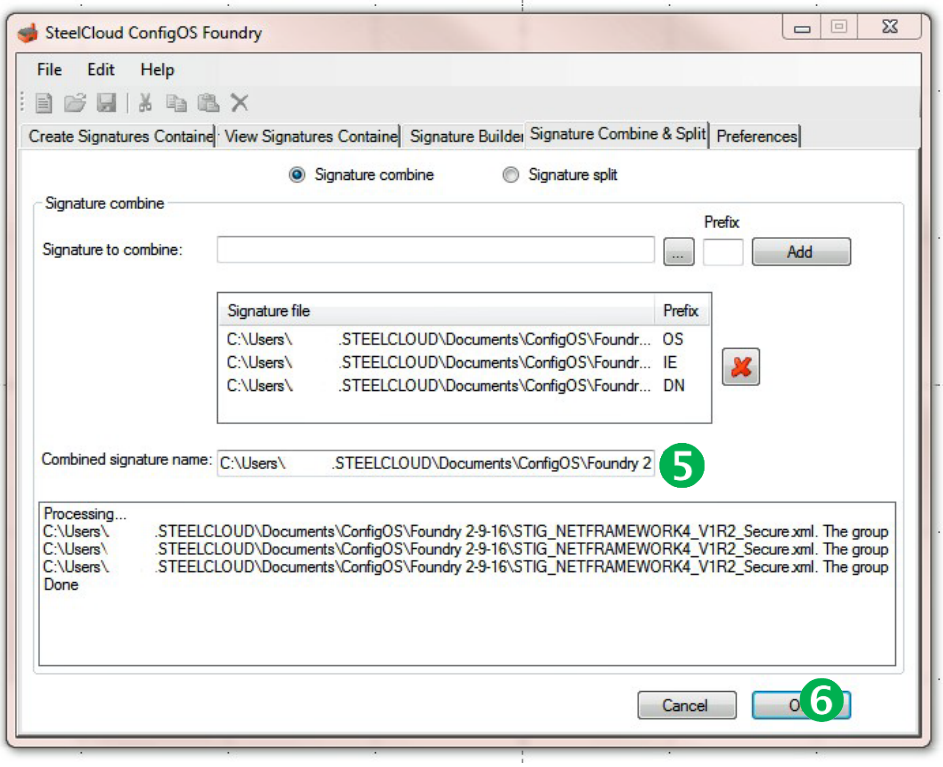
3. Type in a user defined "**Prefix**" and then select "**Add**." **Ensure that the "Prefix" entered for each signature is unique**.

   The Signature file will be added to the combination list.

4. Continue adding individual clear text XML signatures until all required signatures for combination are listed.

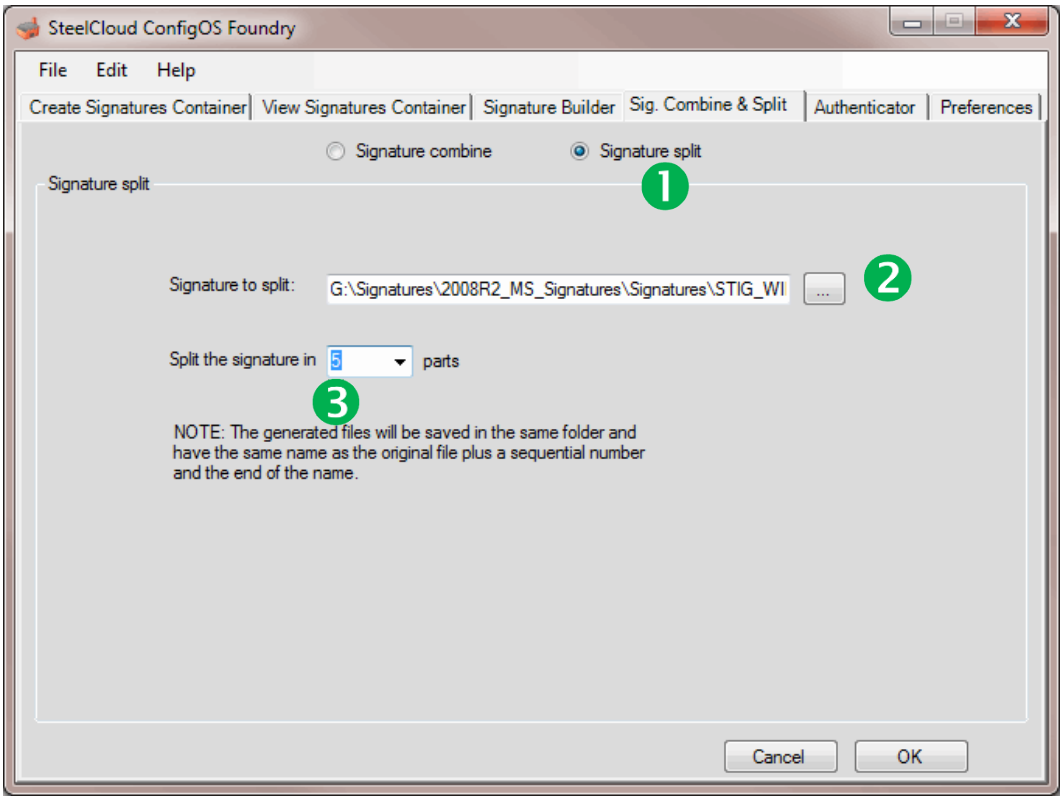
5. Use the file button and enter the location and signature name.

6. Select "**OK**" and the screen will show the progress and the signatures will be combined. The consolidated signature will also be a clear text XML signature that will have to be processed by the foundry in order to be used.



☑ ***Key Concept*** *– The "**Prefix**" is a critical piece of data in this process. When combining multiple signatures into a consolidated signature there is the possibility of having duplication the "V-IDs" which is data that has to be unique. By entering a unique **Prefix** for each signature to be combined, ConfigOS eliminates this possibility duplicate V-IDs. Additionally, it allows the user to be able to trace each control back to its original benchmark signature, visually through the ConfigOS GUI and also on ConfigOS compliance reports.*

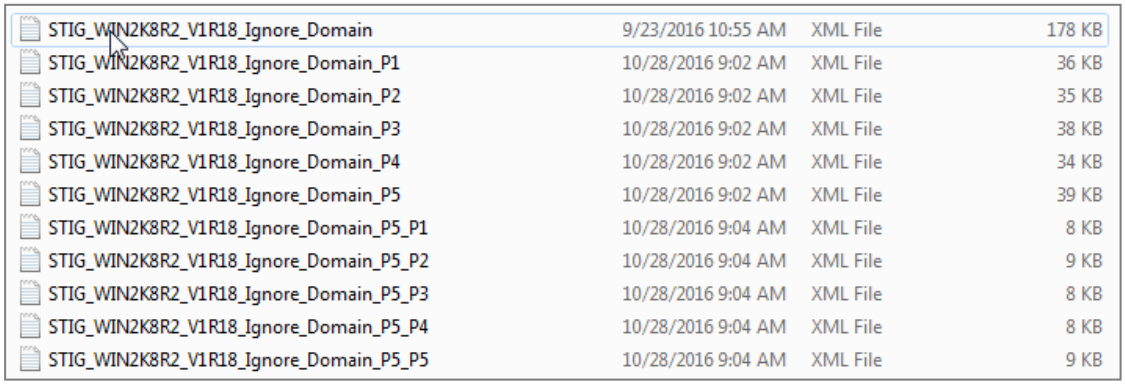
Signature Split has a much different use case than Signature Combine. ConfigOS accelerates the process of hardening controls around an application by being able to quickly apply policy and then immediately roll back the policy if the policy "breaks" the application. It is therefore, extremely helpful to be able to apply smaller segments of a larger policy signature in order to speed the effort necessary to isolate the control(s) that cause operational failures. The ConfigOS Signature Split capability was designed to automate the "splitting" of a large signature into segments in order to be able to apply and rollback subsets of the larger signature.



Signature Split automatically creates multiple smaller clear text XML signatures from a larger clear text XML signature.

1. Ensure that the "**Signature split**" button is selected.
2. Select the clear text XML signatures that you want to split by selecting the "**File**" button and locating the appropriate clear text XML signature.
3. To determine the number of smaller signatures that will be created, use the drop-down control to select from 2 to 5 parts. By selecting "5," the user is indicating that they want 5 smaller signatures to be created from the larger signature. When the user selects the "**OK**" button, the smaller signatures will be automatically created in the same folder with the same file name, appended with a "***_P#***" sequence number for uniqueness.
4. Below is an example of what these smaller sequenced signatures would look like in a file system. Notice that the original Signature was split into five pieces and then the fifth piece was additionally split into five pieces.

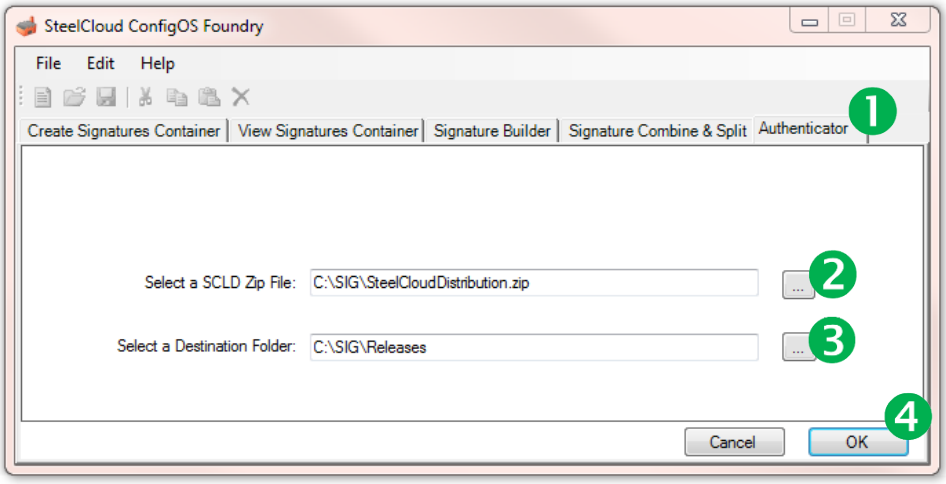
4



☑ ***Key Concept*** *– A user can create as many smaller signatures as required by continuing to split the smaller signatures that have previously been split. ConfigOS sequencing ensures that uniqueness is maintained having all of the resulting pieces appropriately named with sequence numbers.*

L. Authenticator

SteelCloud now releases policy XML Signatures and ConfigOS software (Foundry and Client Manager) as encrypted zip files. This new capability was developed to validate that all SteelCloud content sent to our customers is authentic and has not been compromised.



1 The authenticator tab within the ConfigOS Foundry decrypts and unpacks the encrypted files published by SteelCloud.

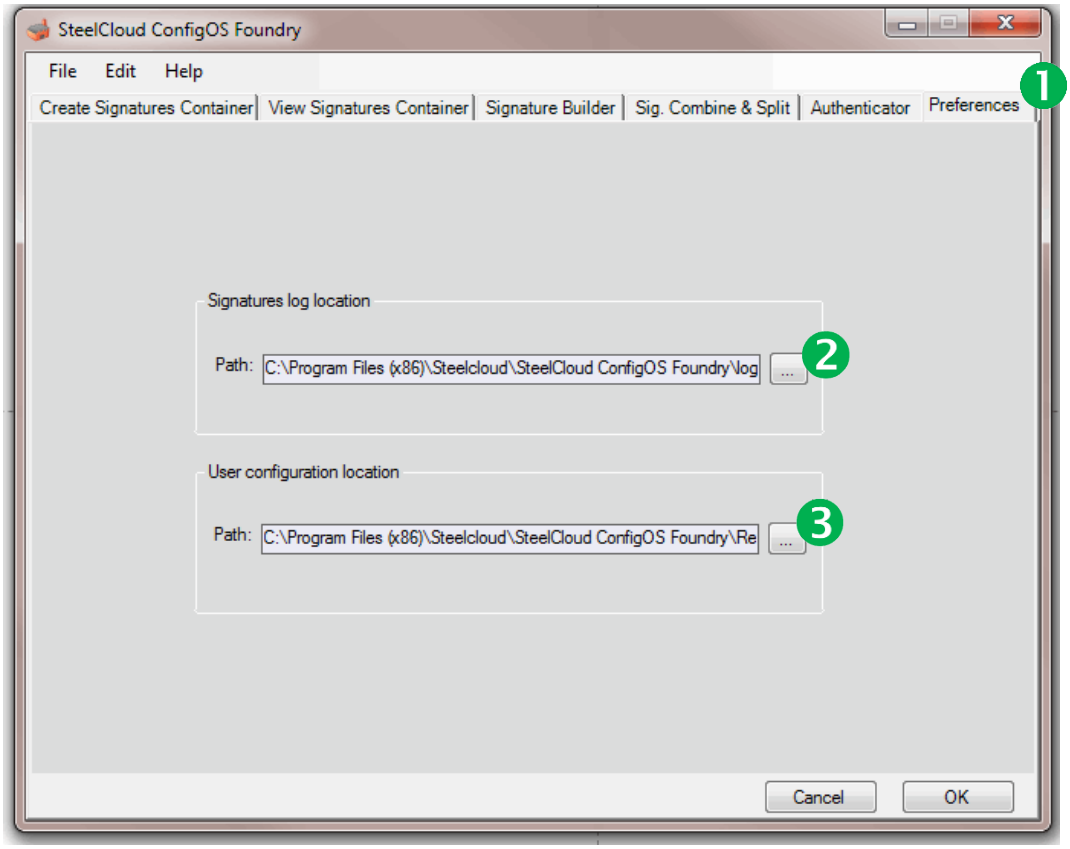
2 Simply locate/select the SteelCloud ZIP file to be decrypted/unpacked.

3 Select the location where the individual decrypted files will be written and select "**OK**." 4

M. Preferences

1. The ConfigOS Foundry "***Preferences***" tab determines the location of two files – Logs and User Configurations.

2. **Logs -** Every time the Foundry creates a new encrypted Signature container, that activity is appended to a Foundry log file. This log file is written to the location specified in the "***Preferences***" tab. **It is important to change the system default location and set up a discrete location for each Foundry deployed to write its log file**.



3. **User Configuration -** The ConfigOS User Configuration file is an XML file that stores default entries that will customize the dropdown box for "***Ignore Reason***." By simply editing the "***Add Value***" line of this XML file, you can standardize the reasons that your organization uses for ignoring or changing controls. The file format is shown below.

```
<?xml version="1.0" encoding="UTF-8"?>
- <UserConfiguration>
  - <Configuration Name="IgnoreReason-Comments">
    - <ValidValues>
        <Add Value="IAW1 - Ignore Application Waiver"/>
        <Add Value="UAW1 - Update Application Waiver"/>
        <Add Value="ISW1 - Ignore Site Waiver"/>
        <Add Value="USW1 - Update Site Waiver"/>
        <Add Value="INW1 - Ignore Not Waiver"/>
        <Add Value="IPO1 - Information Purposes Only"/>
      </ValidValues>
    </Configuration>
</UserConfiguration>
```

N. Appendix

ConfigOS Signatures and Product Contents

1. **Software**
    a. Foundry 1.0.x.x Released Folder
        i. CofigOSFoundrySetup.msi
    b. ConfigOS 2.0.x.x Released Folder
        i. ConfigOSSetup.msi
    c. dotNetFx40_Full_x86_x64.exe (Microsoft .NET 4.6 Stand-Alone installer)

2. **Documentation**
    a. ConfigOS Client Reference Guide v2_x
    b. ConfigOS FoundryReference Guide v1_x vx
    c. Best Practices and Signature Creation
    d. ConfigOS Error Recognition Quick Guide
    e. Sudoers

3. **Signatures**

    a. Systems Folder
        i. Windows 2012 R2 Folder
            1. Windows 2012 DC Folder
                a. STIG_WIN12_VxRx_DC.cxp
            2. STIG_Windows2012_MS_VxRx_STIG
            3. ConfigOS Coverage Win2012.xlsx
            4. CIS_Win2K12R2.cxp
            5. Control Evaluation.cxp
            6. STIG_Win2K12R2_VxRx_NoIgnore_Domain.cxp
            7. STIG_Win2K12R2_VxRx_Ignore_Domain.cxp
            8. STIG_Win2K12R2_VxRx_Ignore_Nondomain.cxp
            9. STIG_Win2K12R2_VxRx_NoIgnore_Nondomain.cxp
            10. Win2012R2Un-Stig.cxp
        ii. Windows 2016 Folder
            1. STIG_Windows2016_MS_V1R1.cxp
            2. STIG_Windows2016_DC_V1R1.cxp
            3. Win2016Un-Stig.cxp

iii. Windows 2008 r2 Folder

1. 2008 DC Folder
    a. STIG_WIN2K8R2_VxRx_DC.cxp
2. Control Evaluation.cxp
3. STIG_Windows_2008_R2_MS_VxRx_STIG
4. ConfigOS Coverage W2K8R2VxRx.xlsx
5. STIG_WIN2K8R2_VxRx_Ignore_Domain.cxp
6. STIG_WIN2K8R2_ VxRx_Ignore_Non-Domain.cxp
7. STIG_WIN2K8R2_VxRxNoIgnore_Domain.cxp
8. STIG_WIN2K8R2_VxRx_NoIgnore_NonDomain.cxp
9. Win2008R2Un-Stig.cxp

iv. Windows 8 Folder

1. STIG_Windows_8_VxRx_STIG
2. ConfigOS Coverage WIN8.xlsx
3. Control Evaluation.cxp
4. STIG_WIN8_VxRx_Ignore_Domain.cxp
5. STIG_WIN8_VxRx_NoIgnore_Domain.cxp
6. STIG_WIN8_VxRx_NoIgnore_NonDomain.cxp
7. STIG_WIN8_VxRx_Ignore_NonDomain.cxp
8. Win8Un-Stig.cxp

v. Windows 7 Folder

1. STIG_Windows_7_VxRx_STIG
2. ConfigOS Coverage WIN7.xlsx
3. Control Evaluation.cxp
4. STIG_WIN7_VxRx_Ignore_Domain.cxp
5. STIG_WIN7_VxRx_NoIgnore_Domain.cxp
6. STIG_WIN7_VxRx_NoIgnore_NonDomain.cxp
7. STIG_WIN7_VxRx_NonDomain.cxp
8. Win7Un-Stig.cxp

vi. IIS Folder

1. IIS7Server.cxp
2. IIS7Site.cxp

vii. SQL Folder

1. SQLServer2012Database.cxp
2. SQLServer2012Instance.cxp
3. MSSQL2012_DatabaseSTIG_CoverageSheet.xlsx
4. MSSQL2012_InstanceSTIG_CoverageSheet.xlsx

viii. Red Hat 6.6 Folder
1. STIG_RedHat_6_VxRx_STIG
2. CIS_RHEL7.cxp Folder
   a. CIS_RHEL7Version1.1.0.cxp
   b. CIS_RHEL7 Coverage Document.
3. Red Hat 6 Folder
   a. ConfigOS Linux CoverageVxRx.xlsx
   b. STIG_CENTOS_VxRx_ignore
   c. STIG_CENTOS_VxRx_Noignore
   d. STIG_RHEL6_VxRx_NoIgnore.cxp
   e. STIG_RHEL6_VxRx_Ignore.cxp
4. Red Hat 7 Folder
   a. STIG_Redhat7_V1R1.cxp
   b. RHEL7 Coverage Document.xlsx
5. Red Hat 5 Folder
   a. STIG_RHEL5_VxRx_Ignore.cxp
   b. STIG_RHEL5_VxRx_NoIgnore.cxp
   c. RHEL5 Coverage Document.xlsx
6. SUSE Folder
   a. STIG_SUSE_V1R7.cxp
   b. SUSE Coverage Document.xlsx

b. Apps Folder
   i. Chrome Folder
      1. STIG_Chrome-VxRx.cxp
      2. ChromeUn-Stig.cxp
   ii. IE10 Folder
      1. STIG_IE10_VxRx.cxp

2. STIG_Microsoft_IE10_V1R12_Manual_STIG Folder
3. ConfigOS Coverage IE10 VxRx.xls

iii. IE11 Folder

1. STIG_IEV11_V*x*R*x*_STIG.cxp
2. STIG_Microsoft_IE11_V*x*R*x*_STIG.cxp
3. ConfigOS Coverage IE11 VxRx.xlsx

iv. Microsoft .NET framework Folder

1. STIG_NETFramework4_VxRx_Secure.cxp
2. STIG_NETFramework4_V*x*R*x*_UnSecure.cxp
3. ConfigOS Coverage Netframework 4 VxR*x*.xlsx

v. MS Office 2010 Folder

1. MicrosoftOffice2010Coverage_VxRx.xlsx
2. MS Office STIG Signatures Folder
   a. MicrosoftOffice2010_V*x*R*x*.xlsx
   b. STIG_MicrosoftOfficeSystem2010_V*x*R*x*_STIG.cxp
   c. STIG_MSAccess2010_V*x*R*x*_STIG.cxp
   d. STIG_MSExcel2010_V*x*R*x*_STIG.cxp
   e. STIG_MSInfoPath2010_V*x*R*x*_STIG.cxp
   f. STIG_MSOneNote2010_V*x*R*x*_STIG.cxp
   g. STIG_MSOutlook2010_V*x*R*x*_STIG.cxp
   h. STIG_MSPowerPoint2010_V*x*R*x*_STIG.cxp
   i. STIG_MSProject2010_V*x*R*x*_STIG.cxp
   j. STIG_MSPublisher2010_V*x*R*x*_STIG.cxp
   k. STIG_MSWord2010_V*x*R*x*_STIG.cxp
3. MS Office Un-STIG Signatures Folder
   a. Access2010Un-Stig.cxp
   b. Excel2010Un-Stig.cxp
   c. InfoPath2010Un-Stig.cxp
   d. Office2010Un-Stig.cxp
   e. OneNote2010Un-Stig.cxp
   f. Outlook2010Un-Stig.cxp
   g. PowerPoint2010Un-Stig.cxp
   h. Project2010Un-Stig.cxp
   i. Publisher2010Un-Stig.cxp
   j. Word2010Un-Stig.cxp
4. MS Office STIG Docs Folder
   a. STIG_MicrosoftAccess2010_V*x*R*x*_STIG.cxp
   b. STIG_MicrosoftExcel2010_V*x*R*x*_STIG.cxp

c. STIG_MicrosoftInfoPath2010_V*x*R*x*_STIG.cxp
d. STIG_MicrosoftOffice2010_V*x*R*x*_STIG.cxp
e. STIG_MicrosoftOneNote2010_V*x*R*x*_STIG.cxp
f. STIG_MicrosoftOutlook2010_V*x*R*x*_STIG.cxp
g. STIG_MicrosoftPowerPoint2010_V*x*R*x*_STIG.cxp
h. STIG_MicrosoftProject2010_V*x*R*x*_STIG.cxp
i. STIG_MicrosoftPublisher2010_V*x*R*x*_STIG.cxp
j. STIG_MicrosoftWord2010_V*x*R*x*_STIG.cxp
k. STIG_Sharepoint_2010_V*x*R*x*_STIG.cxp

vi. MS Office 2013 Folder

1. MicrosoftOffice2013Coverage
2. MS Office STIG Signatures Folder
   a. STIG_MSAccess2013_V*x*R*x*.cxp
   b. STIG_MSExcel_V*x*R*x*.cxp
   c. STIG_MSInfoPath2013_V*x*R*x*.cxp
   d. STIG_MSOneNote2013_V*x*R*x*.cxp
   e. STIG_MSOutlook2013_V*x*R*x*.cxp
   f. STIG_MSPowerPoint2013_V*x*R*x*.cxp
   g. STIG_MSProject2013_V*x*R*x*.cxp
   h. STIG_MSPublisher2013_V*x*R*x*.cxp
   i. STIG_Office2013System_V*x*R*x*.cxp
   j. STIG_Word2013_V*x*R*x*.cxp
3. MS Office Un-STIG Signatures Folder
   a. MSAccess2013Un-Stig.cxp
   b. MSExcel2013Un-Stig.cxp
   c. MSInfoPath2013Un-Stig.cxp
   d. MSOneNote2013Un-Stig.cxp
   e. MSOutlookUn-Stig.cxp
   f. MSPowerPoint2013Un-Stig.cxp
   g. MSProject2013Un-Stig.cxp
   h. MSPublisher2013Un-Stig.cxp
   i. MSSystem2013Un-Stig.cxp
   j. MSWord2013Un-Stig.cxp

4. MS Office STIG Docs Folder
   a. STIG_MicrosoftAccess2013
   b. STIG_MicrosoftExcel2013

c. STIG_MicrosoftInfoPath2013
d. STIG_MicrosoftOfficeSystem2013
e. STIG_MicrosoftOneNote2013
f. STIG_MicrosoftOutlook2013
g. STIG_MicrosoftPowerPoint2013
h. STIG_MicrosoftProject2013
i. STIG_MicrosoftPublisher2013
j. STIG_MicrosoftWord2013

vii. MS Office 2016 Folder

1. MicrosoftOffice2016Coverage_VxRx.xlsx
2. MS Office STIG Signatures Folder
   a. MicrosoftOffice2016_V*x*R*x*.xlsx
   b. STIG_MicrosoftOfficeSystem2016_V*x*R*x*_STIG.cxp
   c. STIG_MSAccess2016_V*x*R*x*_STIG.cxp
   d. STIG_MSExcel2016_V*x*R*x*_STIG.cxp
   e. STIG_MSInfoPath2016_V*x*R*x*_STIG.cxp
   f. STIG_MSOneNote2016_V*x*R*x*_STIG.cxp
   g. STIG_MSOutlook2016_V*x*R*x*_STIG.cxp
   h. STIG_MSPowerPoint2016_V*x*R*x*_STIG.cxp
   i. STIG_MSProject2016_V*x*R*x*_STIG.cxp
   j. STIG_MSPublisher2016_V*x*R*x*_STIG.cxp
   k. STIG_MSWord2016_V*x*R*x*_STIG.cxp
3. MS Office Un-STIG Signatures Folder
   a. Access2016Un-Stig.cxp
   b. Excel2016Un-Stig.cxp
   c. InfoPath2016Un-Stig.cxp
   d. Office2016Un-Stig.cxp
   e. OneNote2016Un-Stig.cxp
   f. Outlook2016Un-Stig.cxp
   g. PowerPoint2016Un-Stig.cxp
   h. Project2016Un-Stig.cxp
   i. Publisher2016Un-Stig.cxp
   j. Word2016Un-Stig.cxp
4. MS Office STIG Docs Folder
   a. STIG_MicrosoftAccess2016_V*x*R*x*_STIG.cxp
   b. STIG_MicrosoftExcel2016_V*x*R*x*_STIG.cxp
   c. STIG_MicrosoftInfoPath2016_V*x*R*x*_STIG.cxp
   d. STIG_MicrosoftOffice2016_V*x*R*x*_STIG.cxp

e. STIG_MicrosoftOneNote2016_V*x*R*x*_STIG.cxp
f. STIG_MicrosoftOutlook2016_V*x*R*x*_STIG.cxp
g. STIG_MicrosoftPowerPoint2016_V*x*R*x*_STIG.cxp
h. STIG_MicrosoftProject2016_V*x*R*x*_STIG.cxp
i. STIG_MicrosoftPublisher2016_V*x*R*x*_STIG.cxp
j. STIG_MicrosoftWord2016_V*x*R*x*_STIG.cxp
k. STIG_Sharepoint_2016_V*x*R*x*_STIG.cxp

viii. Windows Firewall with Advanced Security Folder

1. STIG_WinFirewallCoverage.xlsx
2. STIG_WinFirewallOption1
3. STIG_WinFirewallOption2
4. STIG_WindowsFirewallUn-Stig.cxp

Frequently Asked Questions

1. **I have some questions and would like to talk to a person at SteelCloud - how do I contact SteelCloud?**

   *We are happy to hear from our customers. You can contact us at **info@steelcloud.com**.*

2. **My organization is not part of the DoD, but we would still like to test/use STIG-compliant signatures. Is this version for us?**

   Yes, we have STIG signatures for DoD and non-DoD customers. Give us a call, we would be happy to discuss your options.

3. **How does a customer get updates?**

   We have a secure FTP site where we publish policy XML Signatures, software updates and other documentation. As a customer, you will be given credentials to access this site.

4. **How often are new STIG signatures released?**

   Typically, DISA issues new STIGs once a quarter. SteelCloud will produce new signatures normally within two business days of the DISA STIG release. However, if there is a need for an interim correction, SteelCloud will release new signatures as necessary. Signatures and Signature release information is available through SteelCloud's FTP site.

5. **Why is the Signature creation functionality separated from the standard ConfigOS Client?**

   The Foundry gives organizations the ability to control and protect the production and publishing of signatures. This allows organizations to ensure a high degree of standardization and consistency across their enterprises.

6. **What is the benefit of Encrypting Signatures?**

   Going back to the concept of standardization and consistency, encrypting the signatures ensures that they can be "published" without the worry that they will be tampered with.

7. **What is the operational methodology around deploying multiple Foundries?**

   The ConfigOS Foundry is a control point. Organizations can determine where they want to publish/control signatures – at the enterprise level, by division/component, or by location, domain, etc. ConfigOS give you the flexibility to meet your requirements. For higher volume enterprise signature publishing, multiple Foundries can use the same key and publish signatures to the same community of ConfigOS Client Managers.

8. **What types of information can be included in a signature container?**

   The ConfigOS Signature Container was designed to allow our customers to include any and all information that an end point system administrator might need to perform their job. The ConfigOS Signature Container allows virtually any file type to be used.

9. **How is the Foundry Signature Builder used to harden a system around an application to get to the first 'good' image?**

   The Foundry Builder allows the user to divide a large complex policy signature into smaller pieces. By applying the smaller policy Signature pieces, testing, and utilizing the ConfigOS fallback capability when errors are found, a user can run through 100s of controls and identify the specific one(s) that need to be altered to allow the application to operate normally. The entire process to harden an environment around an application typically takes less than 60 minutes with ConfigOS and the Foundry Signature Builder. And, not only can the process be completed quickly, with ConfigOS, the user will have a complete Signature documenting the exact policy configuration that can be utilized to replicate the results in other lab and production environments.

10. **Are there any additional ConfigOS training materials available from SteelCloud?**

    Yes, SteelCloud has produced a number of ConfigOS training videos that are available at no additional charge to our customers. Training videos are available on our support FTP site.

ConfigOS FoundryEnd User License Agreement

Version 1.5

IMPORTANT—READ CAREFULLY: This End-User License Agreement ("EULA") is a legal agreement between an individual or single entity, or an agency or organization and SteelCloud, LLC (SteelCloud) and other Licensors whose software may be bundled with this product (hereinafter "SOFTWARE"). Clauses will refer to such users as "you" and "yours." The SOFTWARE includes computer software, and may include associated media, printed materials, or electronic documentation. The SOFTWARE is associated with other products which may have their own license agreements or terms of use are governed by such agreements rather than this EULA.

USERS AGREE TO BE BOUND BY THE TERMS OF THIS EULA BY INSTALLING, COPYING, OR OTHERWISE USING THE SOFTWARE. IF YOU DO NOT AGREE TO THE TERMS OF THIS EULA, YOU MAY NOT USE OR COPY THE SOFTWARE, AND YOU SHOULD PROMPTLY CONTACT THE MANUFACTURER FOR INSTRUCTIONS ON RETURN OF THE UNUSED PRODUCT(S) IN ACCORDANCE WITH MANUFACTURER'S RETURN POLICIES.

1. GRANT OF LICENSE. Manufacturer grants you the following rights provided that you comply with all terms and conditions of this EULA:

1.1 You may copy, install, use, access, and display the SOFTWARE only for the number of individual machines for which licenses have been purchased.

1.2 This license may not be transferred without the expressed written consent of SteelCloud.

1.3 You may make a back-up copy of the software. You may use the back-up copy solely for your archival purposes and to reinstall the software.

2. RESERVATION OF RIGHTS AND OWNERSHIP. Manufacturer reserves all rights not expressly granted to you in this EULA. The SOFTWARE is protected by copyright and other intellectual property laws and treaties. Manufacturer owns the title, copyright, and other intellectual property rights in the SOFTWARE. The SOFTWARE is licensed, not sold.

4. LIMITATIONS ON REVERSE ENGINEERING, DECOMPILATION, AND DISASSEMBLY. You may not reverse engineer, decompile, or disassemble the SOFTWARE. You may not disassociate this software from the Manufacturer from which it was originally distributed.

5. RENTAL/COMMERCIAL USE. You may rent, lease, lend or provide others access to the SOFTWARE.

6. TERMINATION. Without prejudice to any other rights, Manufacturer may terminate this EULA if User fails to comply with the terms and conditions of this EULA. In such event user must destroy all copies of the SOFTWARE and all of its component parts.

7. LIMITED WARRANTY. Manufacturer warrants that the SOFTWARE will perform substantially in accordance with the accompanying materials for a period of 3 months from the date that it was purchased. THERE ARE NO OTHER WARRANTIES, EXPRESS OR IMPLIED, EXCEPT TO THE EXTENT REQUIRED BY YOUR LOCAL JURISDICTION'S LAW. FURTHERMORE, EXCEPT TO THE EXTENT REQUIRED BY YOUR LOCAL JURISDICTION'S LAW, THIS WARRANTY DOES NOT ENTITLE YOU TO ANY DAMAGES, INCLUDING BUT NOT LIMITED TO DIRECT DAMAGES, CONSEQUENTIAL DAMAGES OR INDIRECT DAMAGES. THE MANFACTURER'S ONLY OBLIGATION TO YOU UNDER THIS WARRANTY IS, AT ITS OPTION, AND SUBJECT TO APPLICABLE LAW, TO (A) RETURN OF THE AMOUNT PAID (IF ANY) FOR THE PRODUCT(S) IN ACCORDANCE WITH MANUFACTURER'S RETURN POLICIES, OR (B) REPAIR OR REPLACE THE SOFTWARE THAT DOES NOT MEET THIS

LIMITED WARRANTY AND THAT IS RETURNED TO MANUFACTURER. YOU WILL RECEIVE THE REMEDY ELECTED BY MANUFACTURER WITHOUT CHARGE, EXCEPT THAT YOU ARE RESPONSIBLE FOR ANY SHIPPING EXPENSES SPECIFIED IN MANUFACTURER'S WARRANTY REMEDY DOCUMENTATION.

8. DISCLAIMER OF WARRANTIES. The Limited Warranty that appears above is the only express warranty made to you and is provided in lieu of any other express warranties or similar obligations, if any, created by any advertising, documentation, packaging, or other communications. **Except for the Limited Warranty and to the maximum extent permitted by applicable law, Manufacturer provides the SOFTWARE AS IS AND WITH ALL FAULTS, and hereby disclaims all other warranties and conditions, whether express, implied or statutory, including, but not limited to, any implied warranties, duties or conditions of merchantability, of fitness for a particular purpose, of reliability or availability, of accuracy or completeness of responses, of results, of workmanlike effort, of lack of viruses, and of lack of negligence, all with regard to the SOFTWARE, and the provision of or failure to provide support or other services, information, software, and related content through the SOFTWARE or otherwise arising out of the use of the SOFTWARE.**

9. APPLICABLE LAW. This EULA is governed by the laws of the Commonwealth of Virginia.

10. ENTIRE AGREEMENT; SEVERABILITY. This EULA is the entire agreement between you and Manufacturer relating to the SOFTWARE and supersedes all prior or contemporaneous oral or written communications, proposals and representations with respect to the SOFTWARE or any other subject matter covered by this EULA. If any provision of this EULA is held to be void, invalid, unenforceable or illegal, the other provisions shall continue in full force and effect.