



NCCIC

USER MANUAL

The Cyber Security Evaluation Tool (CSET[®]), Version 9.2.3.

User Manual

November 2019

This product was developed by the United States Department of Homeland Security (DHS).

Table of Contents

Introduction to CSET.....	5
Introduction.....	6
Overview.....	8
Disclaimer	12
System Basics.....	13
System Requirements	14
Installation Procedure.....	15
Standalone Install	16
Using the Stand-alone.....	22
Enterprise Install.....	25
Evaluation Preparation	43
Register a User Account.....	45
Import/Export a CSET Assessment	47
Importing a .csetw File.....	48
Importing a .cset File	49
Exporting a CSET Assessment.....	50
Title Bar.....	51
Tools Menu	53
Assessment Documents.....	55
Parameter Editor	56
Protected Features	58
Export to Excel.....	59
Import Module	60
Module Builder.....	64
Create a New Module	65
Add Requirements.....	67
Add Questions	72
Manage Documents	74
Resource Library	75
Search Screen.....	76
Browse Screen.....	78
User Profile.....	82
User Profile.....	84
Change Password	85
Help Menu	86
Accessibility Document.....	88
Keyboard Shortcuts	89
Terms of Use.....	90
About CSET	91
Advisory.....	92
Operation Menus.....	93
Preparation Menu	94
Diagram	96
Questions Menu	97
Results Menu.....	99
Main CSET Window Sections	101
Prepare Section.....	102
CSET Landing Page	103
Assessment Details.....	104
Contacts Management.....	105

Sector and Demographic Information Screen	108
Security Assurance Level (SAL) Selection.....	109
Simple SAL Selection	110
General SAL Selection	113
General SAL – Injury	116
General SAL - Hospital.....	117
General SAL - Death	118
General SAL - Capital Assets	119
General SAL - Economic Impact	120
General SAL - Environmental Cleanup	121
General SAL Considerations.....	122
FIPS 199 SAL Selection	126
Cybersecurity Standard Selection.....	131
CSET Standards and Groupings	133
C2M2 Maturity Indicator Levels	141
CFATS Tiers.....	142
Cybersecurity Framework Description.....	143
Framework Implementation Tiers.....	148
Mode Selection.....	149
Assessment Modes	150
Diagram Screen	152
Diagram Section	153
Diagram Screen Layout.....	154
Diagram Inventory.....	157
Drawing the Network Diagram.....	159
Adding Links.....	163
Adding Text.....	172
Adding Symbols.....	174
Adding Zones.....	182
Using the Multiple Services Component (MSC).	184
Component Types	187
Home Menu Options	194
Home- File Menu	195
Home- Edit Menu	197
Home- View Menu	203
Home- Arrange Menu.....	211
Home- Extras Menu	214
Home- Help Menu	218
Diagram Keyboard Shortcuts.....	219
Format Menu Options	222
Network Deficiency.....	224
Network Analysis Rules.....	225
Assessment Section	228
Assessment Screen	229
Assessment Modes	231
Assessment Screen Questions Mode	232
Assessment Screen Requirements Mode.....	233
Assessment Categories	234
Question Details, Resources, and Comments.....	236
Details Section Question Mode.....	239
Details Section Requirements Mode	241
Supplemental Section	242

Comments Section.....	243
Documents Section.....	244
References Section	246
Observations Section	247
Question Observations.....	248
Feedback Section.....	251
Question Filter.....	252
Component Information.....	254
Network Component Overrides	256
Results Section.....	258
Analysis Screen.....	259
Dashboard in Questions/Requirements Mode.....	262
Control Priorities.....	265
Standards Analysis	268
Standards Summary.....	269
Ranked Categories	271
Results By Category Single Standard	273
Results by Category Multiple Standards	274
Category Rankings.....	275
Components Summary.....	278
Ranked Categories	279
Results by Category.....	280
Component Type	281
Network Warnings.....	282
Reports Section.....	283
Executive Summary, Overview, and Comments Screen.....	284
Report Builder.....	285
Executive Summary Report.....	287
Site Summary Report	289
Site Detail Report.....	292
Site Cyber Security Plan	293
Observation Tear Out Sheets	295
Submit Feedback.....	296
Initiation Scenarios.....	297
Glossary	301
Frequently Asked Questions (FAQs)	305
CSET Revision History.....	307

Introduction to CSET

This section will help the user better understand the Cyber Security Evaluation Tool (CSET[®]), its background, and purposes.

Introduction

The Cyber Security Evaluation Tool (CSET[®]) provides the following:

1. A framework for analyzing cybersecurity vulnerabilities associated with an organization's overall industrial control system (ICS) and information technology (IT) architecture;
2. A consistent and technically sound methodology to identify, analyze, and communicate to security professionals the various vulnerabilities and consequences that may be exploited by cyber means;
3. The means for the user to document a process for identifying cybersecurity vulnerabilities; and
4. Suggested methods to evaluate options for improvement based on existing Standards and recommended practices.

Background

The Department of Homeland Security (DHS) developed CSET for asset owners with the primary objective of reducing the risk to the nation's critical infrastructure. Control systems are defined as electronic devices that control physical processes and as such, are a crucial element in the protection of our nation's infrastructure.

CSET is a web-based tool that guides users through a step-by-step process to collect facility-specific information addressing topics such as hardware, software, administrative policies, and user obligations. It then compares that information to relevant security Standards and regulations, assesses overall compliance, and provides appropriate recommendations for improving cybersecurity posture. The tool pulls its recommendations from a collection of the best available cybersecurity Standards, guidelines, and practices. Where appropriate, recommendations are linked to a set of actions that can be applied to enhance cybersecurity controls.

Objectives and Benefits

The primary objective of CSET is to reduce the risk of cyber attacks by identifying potential cybersecurity vulnerabilities within a system or an organization. CSET implements a simple, transparent process that can be used effectively by all sectors to perform an evaluation of any network. It offers the following benefits:

- Provides a repeatable and systematic approach for assessing the cybersecurity posture of a system, network, site, or facility.
- Provides a comprehensive evaluation and comparison to existing industry Standards and regulations.
- Combines the ICS and IT security knowledge and experience of many organizations.
- Assists in the identification of potential vulnerabilities in the network design and security policies.
- Provides guidelines for cybersecurity solutions and mitigations.
- Provides access to a centralized repository of cybersecurity requirements.
- Provides an opportunity for dialogue on security practices within the user's facility.

Limitations of this Tool

The tool has a component focus rather than a system focus. Therefore, network architecture analyses, including network hardware and software configuration analyses, will be limited to the extent that they are defined by programmatic and procedural requirements.

CSET is not a risk analysis tool; it will not create a detailed risk assessment.

Most importantly, CSET is only one component of a comprehensive control system security program. A security program based on a CSET assessment alone must never be considered complete or adequate.

User Qualifications

CSET assessments cannot be completed effectively by any single individual. A cross-functional team consisting of representatives from multiple company areas is essential. The representatives must be subject matter experts with significant expertise in their respective areas. No one individual has the span of responsibility or knowledge to be able to fully and accurately answer all the questions provided by the CSET tool.

Overview

The Cyber Security Evaluation Tool (CSET[®]) is a software tool for performing cybersecurity assessments of an organization's enterprise and industrial control cyber systems. It was designed to help asset owners identify vulnerabilities and improve the organization's overall cybersecurity posture by guiding them through a series of questions that represent network security requirements and best practices. The presented requirement questionnaires are based on selected industry Standards, common requirements, and the network diagram (or network topology and architecture).

CSET Framework

The underlying framework for CSET includes:

- Analysis and user interface tools to assist in the evaluation of an ICS,
- A knowledge base of ICS cybersecurity requirements, regulations, and practices, and
- A collection of solutions to help mitigate vulnerabilities.

Basic Evaluation Process

Form the Assessment Team

Prior to beginning the assessment, form a subject matter expert team. Teams typically include representation from senior management, business, operations, IT, ICS, and security. The assembled team is responsible for determining the evaluation levels and answering specific, detailed questions on the control system and security configuration.

Familiarity with the tool will improve and speed up the assessment process. Anyone in the organization who has had training or experience with the tool should be included on the team. Alternately, the primary user should spend some time using the tool with test-only or dummy data prior to commencement of the team activity.

Documents that may be referenced should be gathered prior to the assessment. Useful reference materials include information relating to operations, maintenance, physical security, cybersecurity, and hazardous materials.

Launch CSET

There is more than one way to use an instance of CSET. Whether you are using a web instance, standalone, or a enterprise installation.

Web Instance

If you are using a public, web instance then you will need to register for a CSET account.

Register for a CSET Account

Register for CSET by first installing CSET. The CSET installation will be on your local desktop. If it is installed locally click the icon to start, if your CSET installation is an Enterprise or company installation see your company CSET administrator for the URL.

After installation navigate to the CSET home page. Below the login is a link that says "Register New User Account". See more on registering a new account at [Register a User Account](#). A new assessment can be started from the user's landing page by clicking the "Start New Assessment" button.

New Assessment

Figure: New Assessment button

Standalone

For more information on the standalone build, see the [standalone install](#) help section.

Enterprise

For more information on the enterprise build, see the [enterprise install](#) help section.

Add Site Information

Begin the assessment by filling out assessment details. This includes the assessment name and date, information on the subject system, points of contact, and a description of the assessment. Such information will be helpful when referring to the assessment months or years later.

For more information, see the [Assessment Details](#) help section.

The figure below graphically depicts the next steps of the self-assessment process. A brief summary of the steps is provided below.

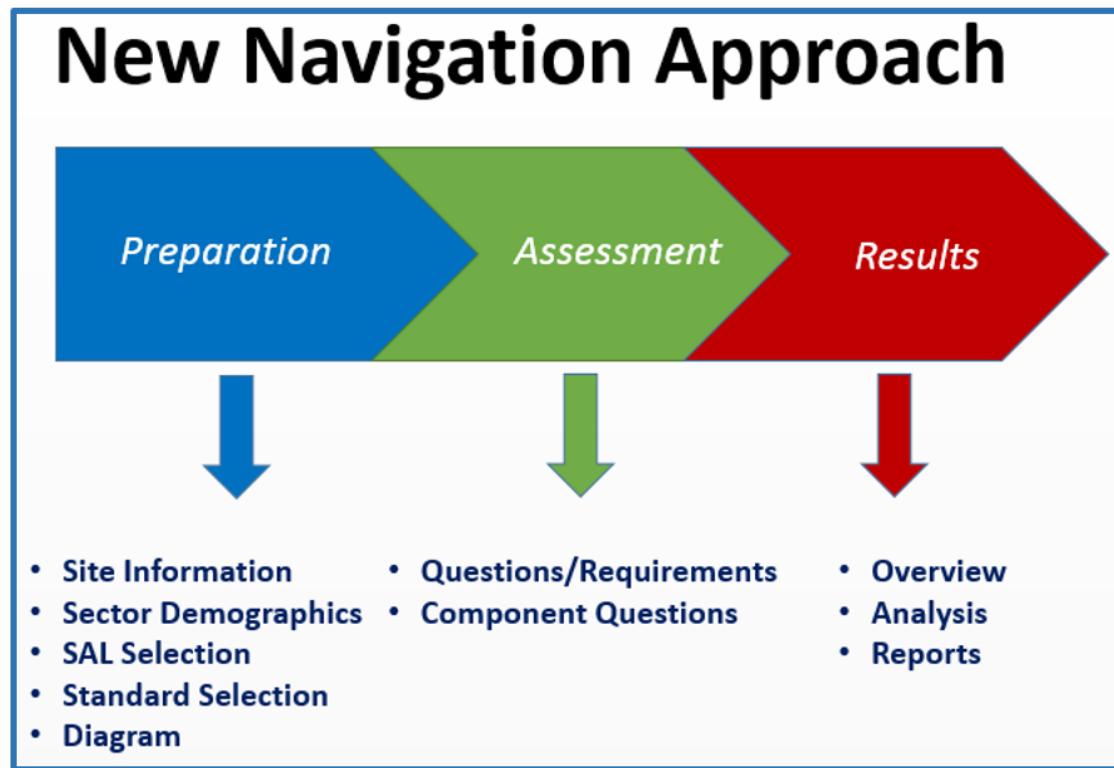


Figure: CSET process

Preparation

Site Information

The first part of the assessment preparation process is to provide specific information about the assessment including who was responsible, when it occurred, what sites or facilities were involved, and both descriptive and summary information.

Sector Demographics

Providing sector and demographic information allows CSET to suggest typical Standards that drive assessment questions.

Security Assurance Level (SAL) Selection

The SAL value selected will limit the required questions to only those related to the selected level. The SAL value is also used in the ranking of missed questions.

The system requires that the user identify a SAL, and multiple options are provided to determine what the SAL should be. The user may bypass the guidance screens and directly select the SAL. The user may employ the General SAL guidance (consequence based) or the Federal Information Processing Standard (FIPS) 199 SAL guidance (based on FIPS 199 and National Institute of Standards and Technology (NIST), Special Publication (SP) 800-60).

For more information about Security Assurance Levels or SALs, see the [Security Assurance Level \(SAL\) Selection](#) help section.

Standard Selection

Included on the Cybersecurity Standard Selection screen is a list of Standards and guides applicable to the mode options. The list of choices will vary depending on which mode is selected. Advanced users will have the option to select one or more Standards against which they would like to be evaluated.

For more information about Standards, see the [Standards Screen](#) help section.

Create Diagram

CSET provides a versatile diagramming tool to create a network diagram of the system being assessed. Diagram allows a system and/or network to be modeled in detail using predefined templates and stencils specifically used in industry standards. Once the diagram has been developed, attribute data can be assigned that will enhance the visual presentation, allow grouping and layers, and provide input to the analysis and question ranking. Simple network analysis is available within the tool and is provided in the reports and the Analysis screen.

For more information about Diagram, see the [Diagram Screen](#) help section.

Assessment

Questions

Once a Standard has been selected, CSET will generate a set of assessment questions that can be accessed from the Assessment screen. All questions will be answered as either Yes, No, Not Applicable (NA), or through an Alternate text field (ALT).

If the "Requirements" mode is selected, the questions will be presented as explicit requirements from the selected industry Standard.

The process of answering questions is tedious but straightforward. As a team, start with Question 1 and continue through each subject area or category until all questions have been discussed and answered.

Component Questions

After the user builds the network diagram, CSET generates the component questions based on component types and which components were marked as unique. The questions are grouped so that a default question can apply to a range of types. The system also allows overrides to an answer based on either the type or the individual component.

Results

Dashboard

The Results dashboard shows the basic score or results of the assessment at a glance. The overview shows 2 scores: (1) the overall score, and (2) a standards based score. It also shows charts for Assessment Compliance, Top Ranked Categories, Standards Summary, and Component Summary.

Analysis

Assessment results can be reviewed in two locations: the analysis charts and the printed reports. The first is from the Analysis Screen containing charts and tabular data that present both summary and detailed information about how well users are doing and where they need to improve, including rankings for questions by category and the questions themselves.

The second way to view assessment results is through a set of printed reports.

For more information about Analysis, see the [Results](#) help section.

Reports

The reports provide the details and scores of the assessment and allow for printing and publishing the assessment information, including summary charts and lists. Reports can help the user clearly understand where weaknesses are and where improvements should be made.

From the executive to the site summary and the site detail reports, each report provides increasing levels of detail. Finally, the security plan report provides a template for documenting the required cybersecurity controls and the degree to which they are met. The printable reports contain charts, lists, and detail information found on the analysis screen.

For more information about Reports, see the [Reports](#) help section.

Additional Actions

Utilize Assessment Documents

CSET gives users the opportunity to collect and store all documents relevant to an assessment. This collection may be accomplished in two ways. First, all questions can have one or more documents associated with them indicated in the documents section of the details and resources link under each question. The second way is accessed from the Assessment Documents link accessed from the Help menu. The Document Library screen lists all documents currently associated with the assessment.

For more information, see the [Assessment Documents](#) help section.

Utilize Resource Library

The Resource Library is a source for additional cybersecurity documentation. It is accessed from the [Title Bar](#) on the main CSET window. The Resource Library contains reference materials to answer many technical or policy questions and aid in the creation and maintenance of a comprehensive cybersecurity program.

For more information, see the [Resource Library](#) help section.

Protect Information

Data Recovery

CSET continuously saves data that is entered. If CSET is closed or the browser restarts all the entered data will be stored automatically.

Disclaimer

The following disclaimer will be seen when installing CSET:

"The analysis, data, and reports in CSET® are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. In no event shall the United States Government or its contractors or subcontractors be liable for any damages, including but not limited to, direct, indirect, special, or consequential damages and including damages based on any negligence of the United States Government or its contractors or subcontractors, arising out of, resulting from, or in any way connected with this report, whether based on warranty, contract, tort, or otherwise, whether injury was sustained from, or arose out of the results of, or reliance upon the report."

"DHS does not endorse any commercial product or service, including the subject of the assessment or evaluation in this report. Any reference to specific commercial products, processes, or services by trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by DHS."

"The display of the DHS official seal or other DHS visual identities on this report shall not be interpreted to provide the recipient organization authorization to use the official seal, insignia or other visual identities of DHS. The DHS seal, insignia, or other visual identities shall not be used in any manner to imply endorsement of any commercial product or activity by DHS or the United States Government. Use of the DHS seal without proper authorization violates federal law (e.g., 18 U.S.C. §§ 506, 701, 1017) and is against DHS policies governing usage of the seal."

"The report is prepared and intended for internal use by the organization that made the request. The contents of this report may be subject to government or private intellectual property rights. To request distribution of this report outside the organization for which it was prepared, contact the CSET Program Office. The contents of this report may be reproduced or incorporated into other reports, but may not be modified without the prior express written permission of the CSET Program Office."

System Basics

This section describes system requirements, installation instructions, and recommendations on how to go about preparing for the cybersecurity evaluation.

System Requirements Local Installation

It is recommended that users meet the minimum system hardware and software requirements prior to installing CSET. This includes:

- Pentium dual core 2.2 GHz processor (Intel x86 compatible)
- 6 GB free disk space
- 4 GB of RAM
- Microsoft Windows 7 or higher
- Microsoft .NET Framework 4.7 Runtime (included in CSET installation)
- SQL Server 2012 Express LocalDB (included in CSET installation)
- IIS Express 8 (included in CSET installation)

System Requirements Enterprise Installation

It is recommended that users meet the minimum system hardware and software requirements prior to installing CSET. This includes:

- Pentium dual core 2.2 GHz processor (Intel x86 compatible)
- 8 GB free disk space
- 4 GB of RAM
- Microsoft Windows Server 2012 Edition or higher recommended
- Microsoft .NET Framework 4.7 Runtime
- SQL Server 2012 or higher recommended
- Internet Information Server (IIS)

Other Items of Note:

- For all platforms, it is recommended the user upgrade to the latest Windows Service Pack and install critical updates available from the Windows Update web site to ensure the best compatibility and security.
- If the install must be made through physical media, a USB port will be required.
- If desired, HTML reports will need to be converted to PDF using an external utility.
- If the Microsoft .NET Framework 4.6.0 Runtime is not available on the user's computer, CSET will automatically install it, which can add several minutes to the installation time. (For local installation)

Installation Procedure

CSET has two different methods of install.

Select an option below to learn more.

Standalone Install

Double-click on the CSETStandAlone program.
The User Account Control dialogue will come up. Select "Yes".

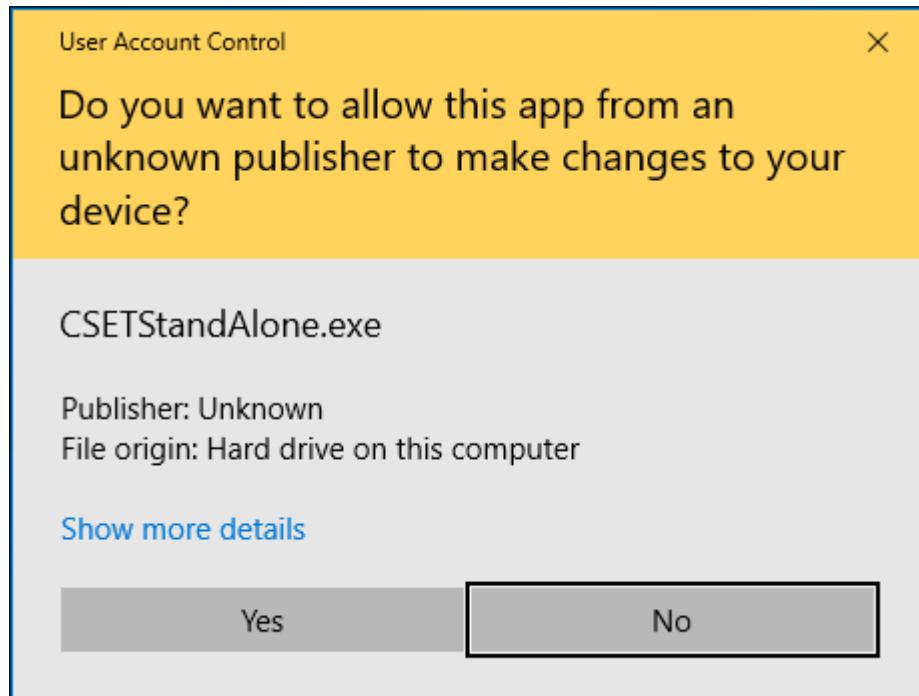


Figure: User Account Control box

A CSET dialogue will open asking if you want to install CSET Desktop. Select "Yes".

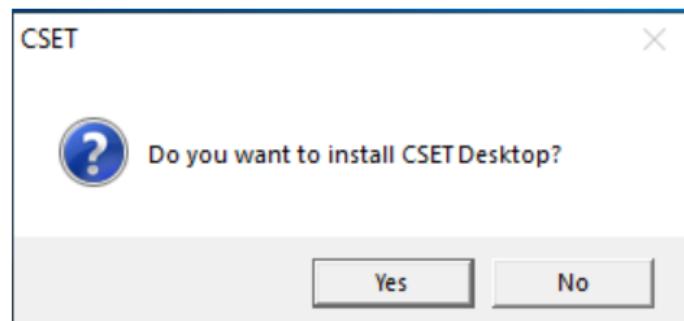


Figure: Install dialogue

The program will begin extracting.
After extracting a CSET setup dialogue will open. Click "I agree to the license terms and conditions" and then select "Install".

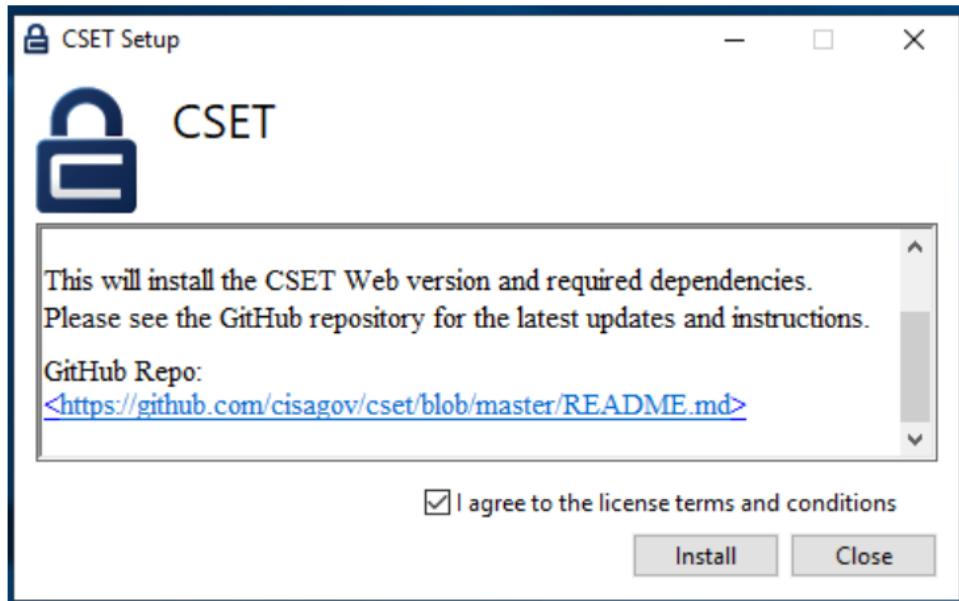


Figure: CSET Setup

CSET will begin to install. If the user doesn't have SQL Server 2012 Express, CSET will install it. The SQL Server 2012 Express Setup dialogue will open. Click "Next" and then select "Install".

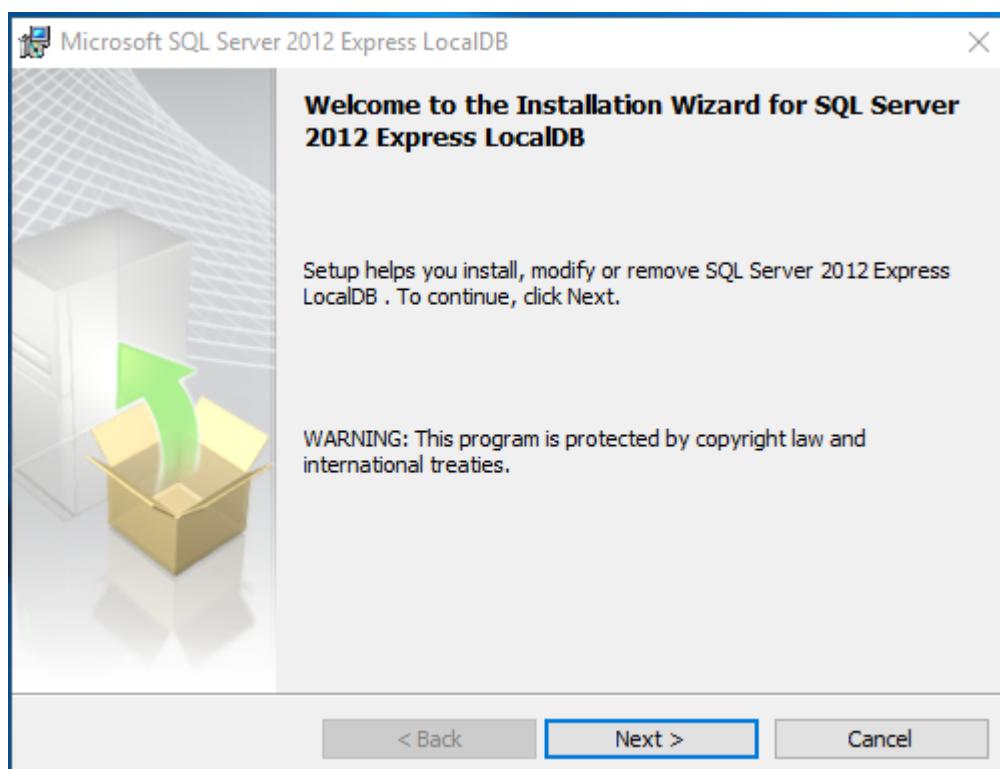


Figure: SQL Server setup

If the user doesn't have IIS 10.0 Express, CSET will install it. The IIS 10.0 Express Setup dialogue will open. Click the check box to confirm that you "...accept the terms in the License Agreement", and then select "Install".

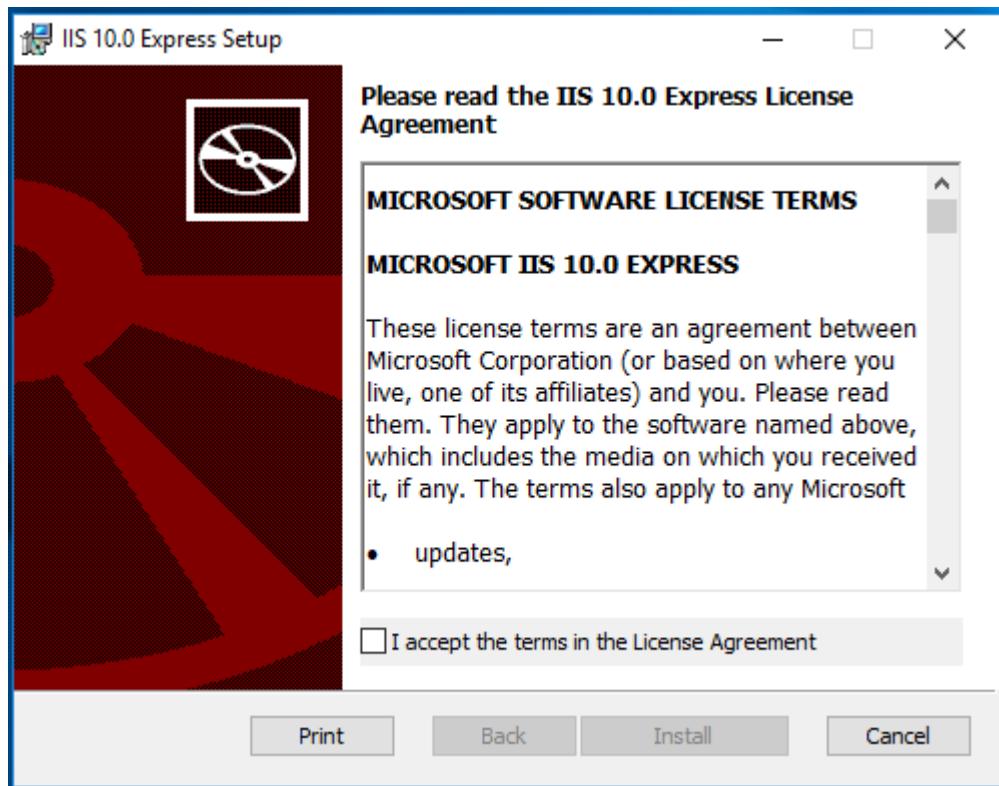


Figure: IIS Setup

IIS will install. Select “Finish” when it completes.

The CSET setup wizard will open to walk the user through the install process. Select “Next”.

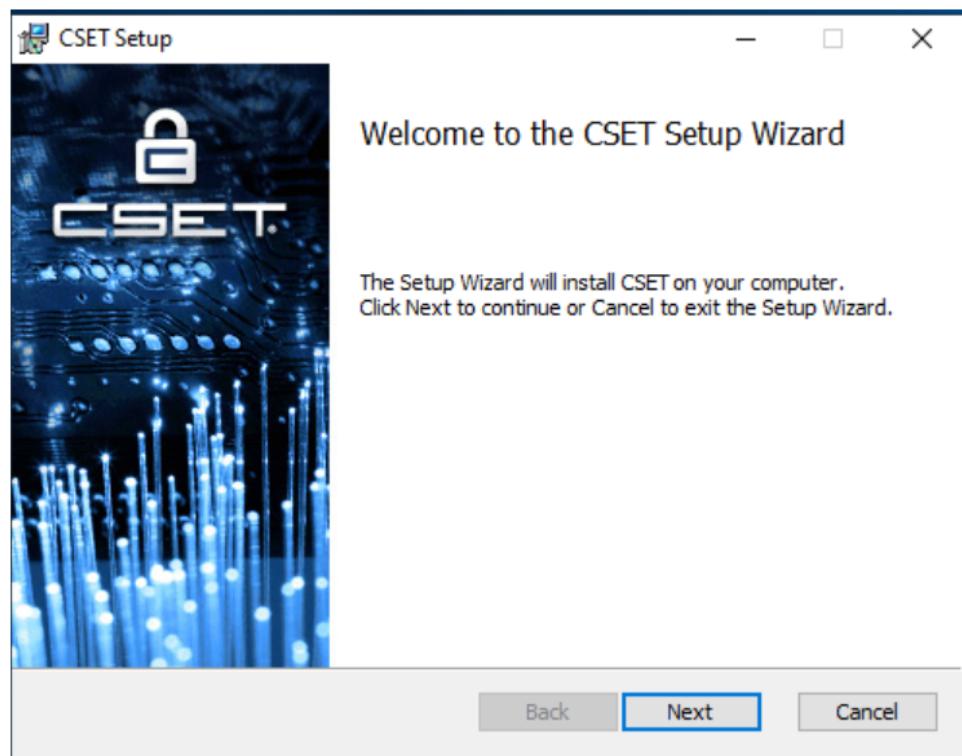


Figure: Setup Wizard

A disclaimer will open. Read through and then click the box “I read the disclaimer”, and select “next”.

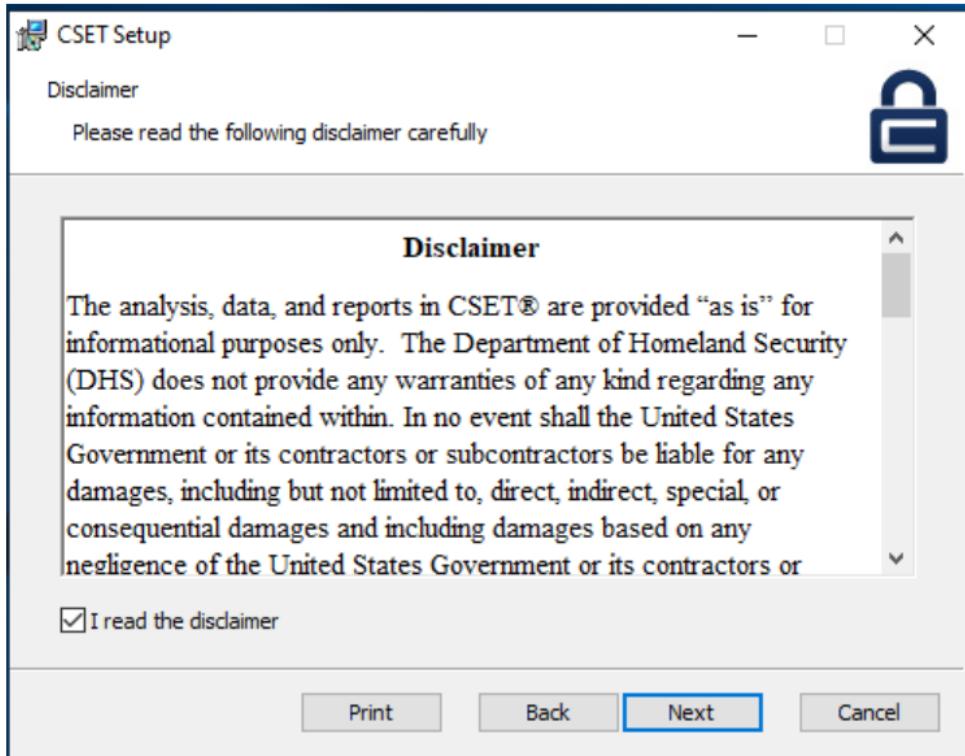


Figure: Disclaimer

CSET will choose a default folder to install CSET to, but you can change this in the Destination Folder dialogue. Select "Next".

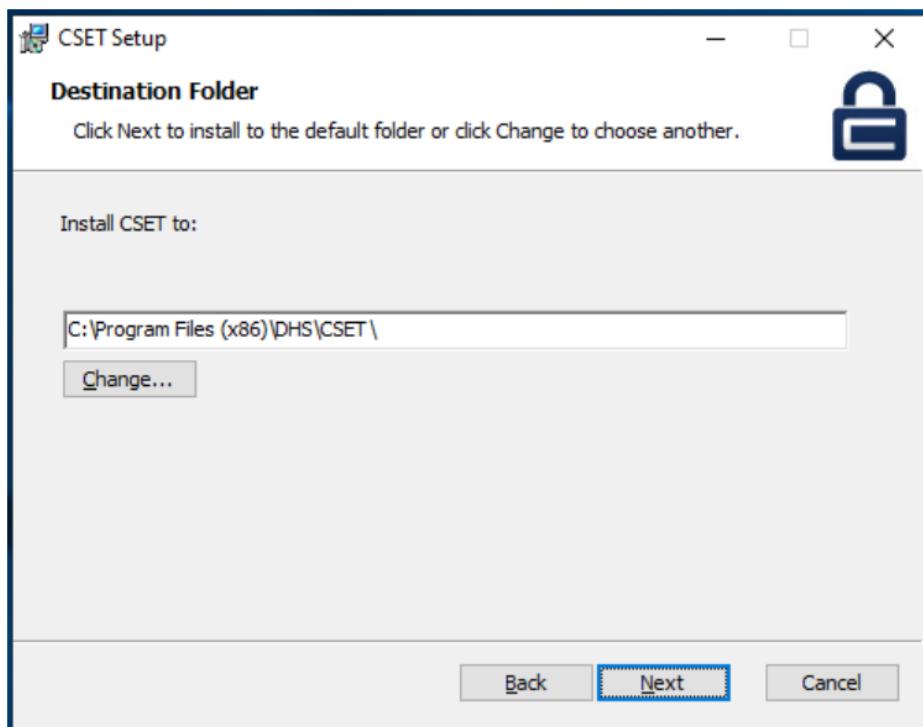


Figure: Destination Folder

The CSET Installer will show that it is ready to install, select "Install".

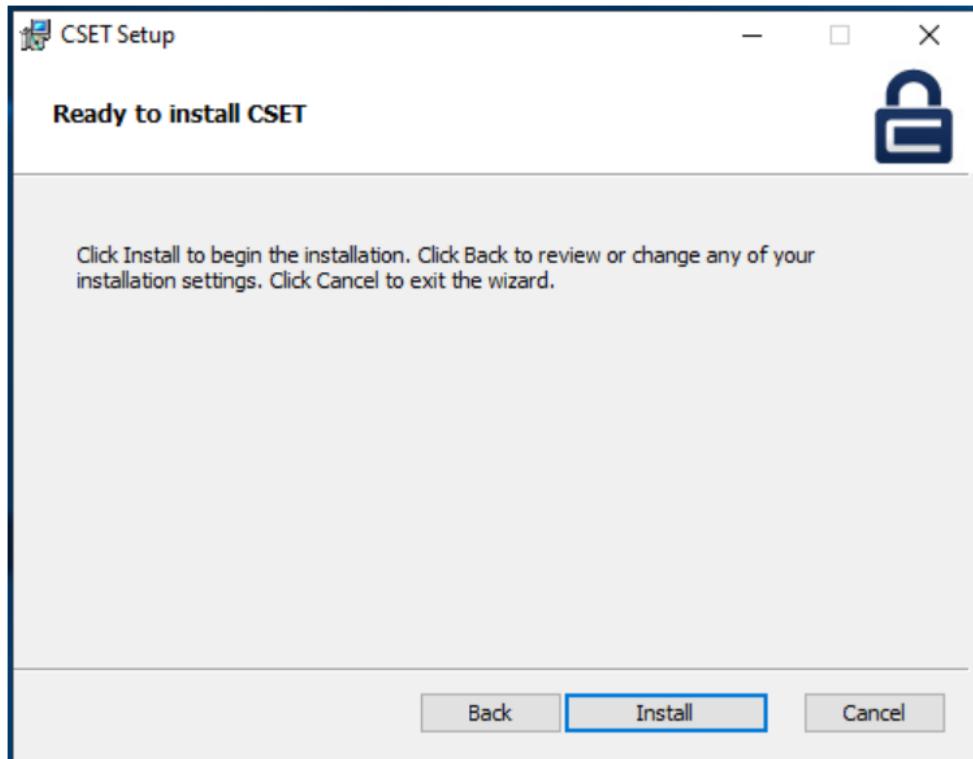


Figure: Ready to install

CSET will be installed. Make sure that the “Launch CSET when setup exists” box is checked, and select “Finish”. The user should see a setup successful dialogue, and then have an option of how they want to open the app. For this example, Edge was used.

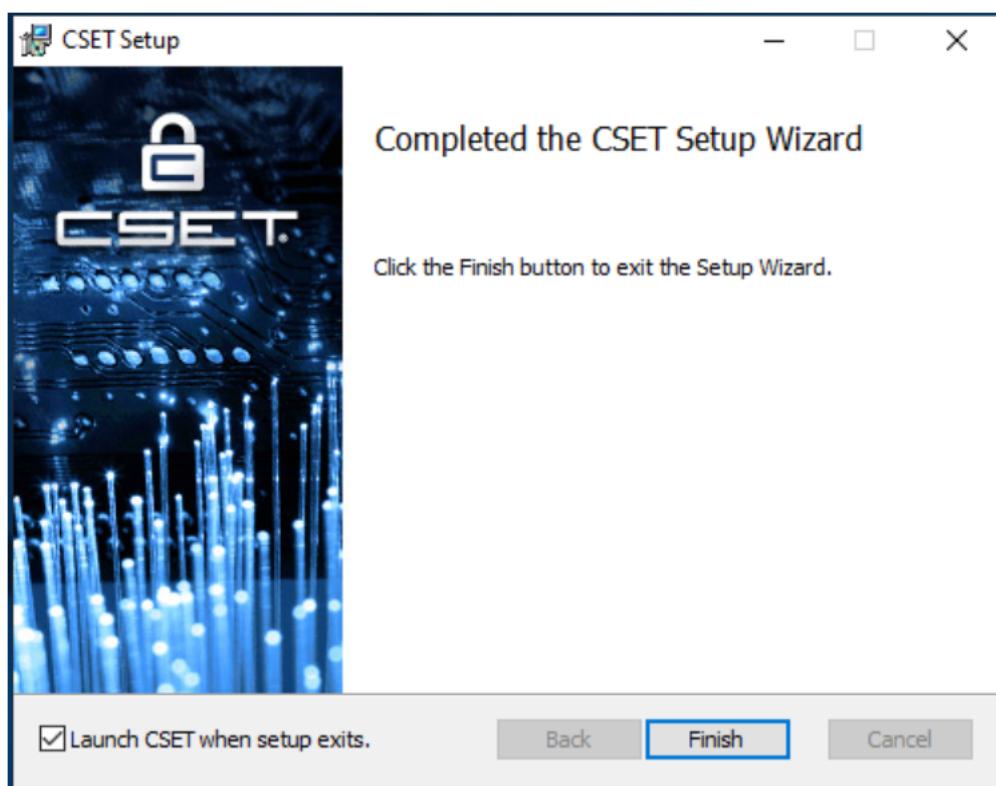


Figure: Setup successful

The user has access to CSET as Local User. The Local Installation ribbon is visible at the top of the screen. They can see their landing page with no assessments at this time.

Welcome to CSET

To get started, select from one of the options below:

 Start a New Assessment Import an existing assessment

The Cyber Security Evaluation Tool (CSET®) is a Department of Homeland Security (DHS) product that assists organizations in protecting their key national cyber assets. It was developed under the direction of the DHS National Cybersecurity Assessments and Technical Services team (NCATS) by cybersecurity experts. This tool provides users with a systematic and repeatable approach for assessing the security posture of their cyber systems and networks. It includes both high-level and detailed questions related to all industrial control and IT systems.



Figure: Local install landing page

Using the Stand-alone

There are a few things users should know in regards to the stand-alone install of CSET.

Using the CSET System Tray Application

The CSET system tray app will be available in the user's task bar. To use it click the CSET icon .

The user will have the option to Open CSET Web, Start CSET Web, Stop CSET Web, Configure/Status, or Exit.

Selecting "Open CSET Web" will open a web instance of CSET.

Selecting "Start CSET Web" will run the application. If the application is already running the Start CSET Web option will not be available, and the user should see in the Configure/Status that the Status is "Running".

Selecting "Stop CSET Web" will end the application.

Selecting "Configure/Status" will open the CSET Web- Local Configuration and Status box. The user can utilize this to change their port, check the status of the application, or check the output log.

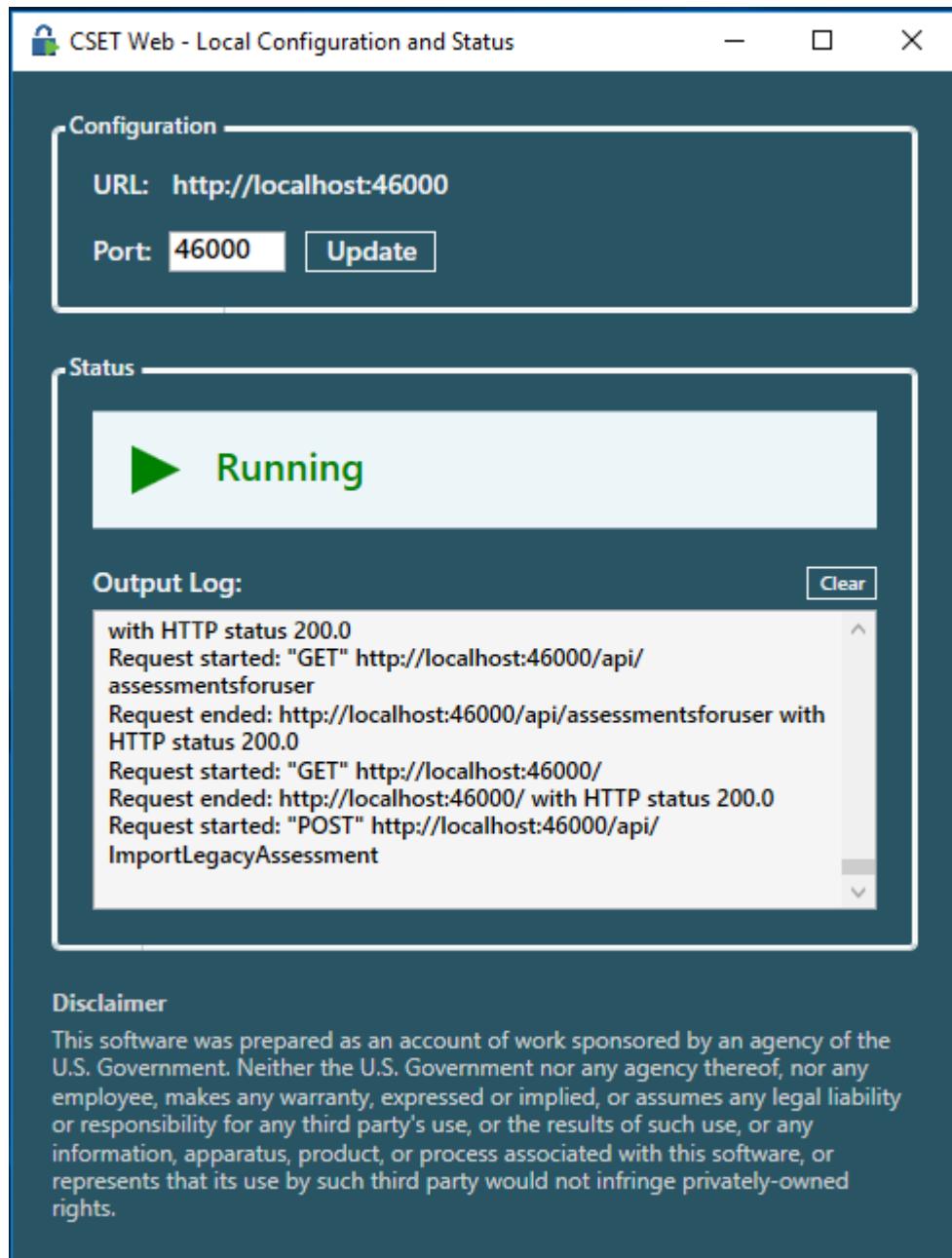


Figure: Local Configuration and Status box

Selecting the "Exit" option will close the CSET system tray application menu.

Differences Between the Local and Web Versions of CSET

When using the stand-alone a gold ribbon that says "Local Installation" is displayed. See the figure below.

In the User Profile menu there is only the option to go to "My Assessments". User's can't alter their profile information while in stand-alone mode, so instead of seeing their name they will see "Local User".

Emails are not available while in stand-alone. All email functionality is in the web-based version of CSET.

CSET

localhost:46000/home/landing-page

Local Installation

CSET Tools Resource Library Local User Help

My Assessments

New Assessment Import

Assessment Name	Last Modified	Primary Assessor	Status
New Assessment	08-Nov-2018	Local User	



^

Figure: Stand-alone landing page

Enterprise Install

2

Introduction

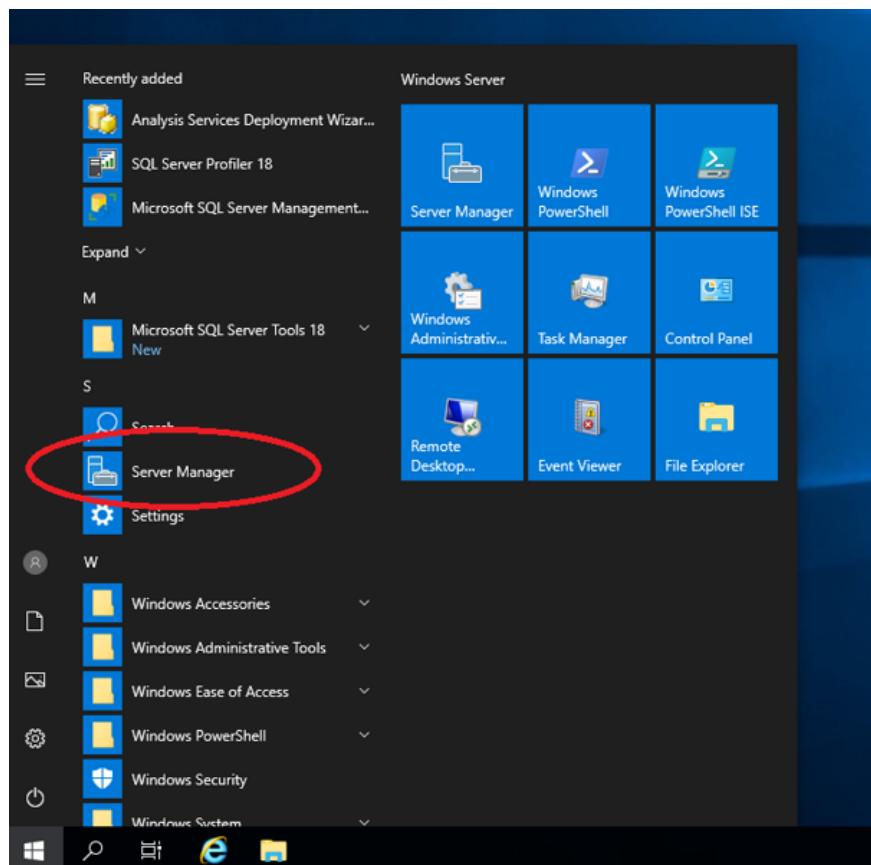
This document is provided to assist users in navigating the basics of CSET Enterprise. Within this document, users will find step-by-step directions for installation, configuration, and setup, as well as links to various resources to assist in this process.

Prerequisites / Necessary Files

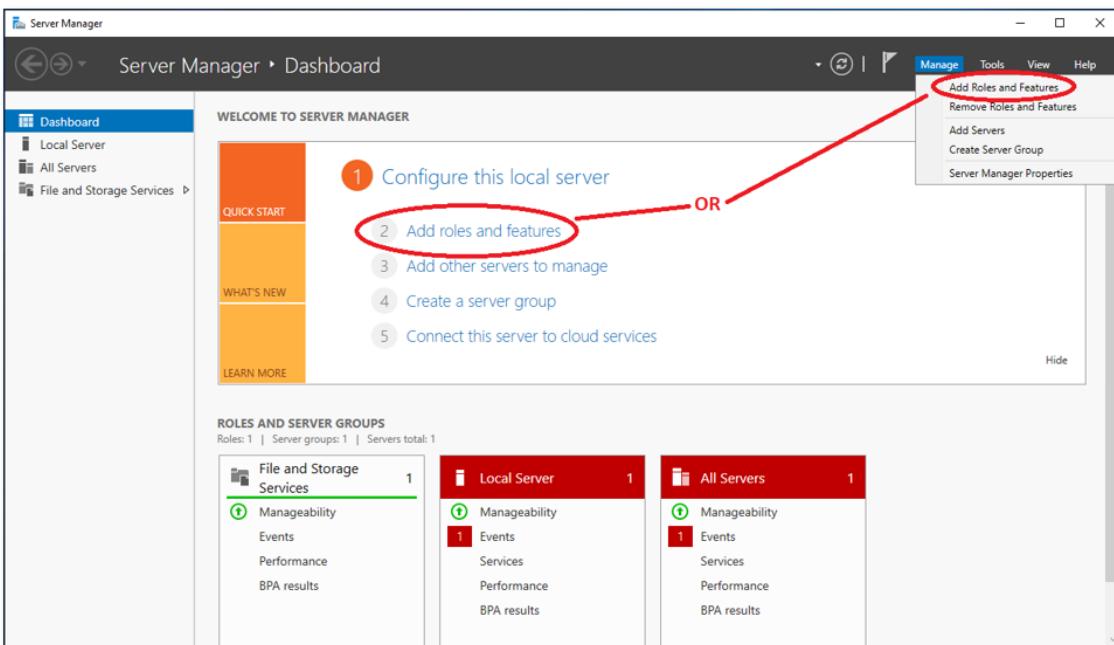
1. Download the “Enterprise Distribution Files” from the CSET GitHub page here: <https://github.com/cisagov/cset/releases/tag/9.2.2enterprise>. Click the “AddUser.zip” and “CSET9.2.2.zip” links to download the two files you need. Once the download is complete, you will need to extract the folders.
2. We will be using Microsoft SQL Server 2016 for this setup. If you need to, you can download the Express version from Microsoft directly here: <https://www.microsoft.com/en-us/download/details.aspx?id=56840>
 - a. CSET requires your server to have the URL Rewrite Module installed as well. This can be downloaded directly from Microsoft here: <https://www.microsoft.com/en-us/download/details.aspx?id=47337>
3. If you are using an SQL Server, download and install Microsoft “SQL Server Management Studio (SSMS)” here: <https://docs.microsoft.com/en-us/sql/ssms/download-sql-server-management-studio-ssms?view=sql-server-ver15>

Install IIS

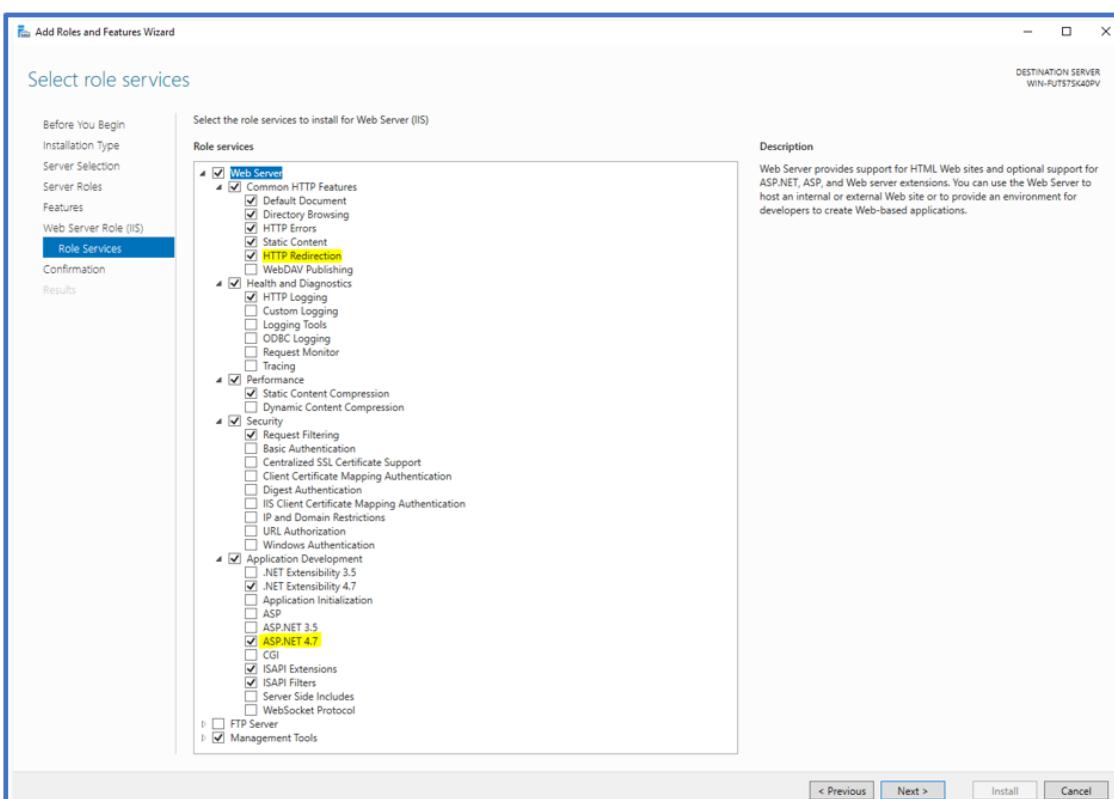
1. On your Windows Server, open the “Server Manager” application (see below).



2. Click “Add Roles and Features.” This should open the Roles and Features Wizard that will guide you through the installation process.



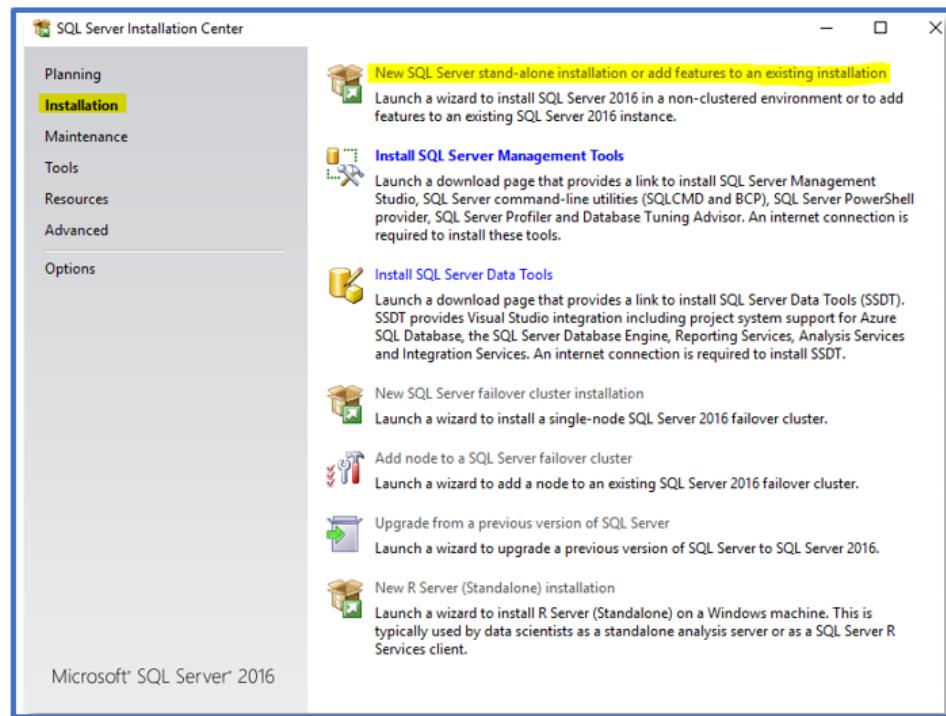
- Installation Type** – This should default to “Role-based or feature-based installation.” If it does not, please select this option.
- Server Selection** – Choose the server you plan on running CSET® on.
- Server Roles** – Select the “Web Server (IIS)” check box. Add any features the program prompts you for.
- Features** – The defaults will work just fine for running CSET®, however you may add any additional features you wish.
- Web Server Role (IIS)** – Click “Next.”
- Role Services** – Under Common HTTP Features, select “HTTP Redirection.” Under Application Development, select “ASP.NET 4.7” and add any features the program prompts you for.



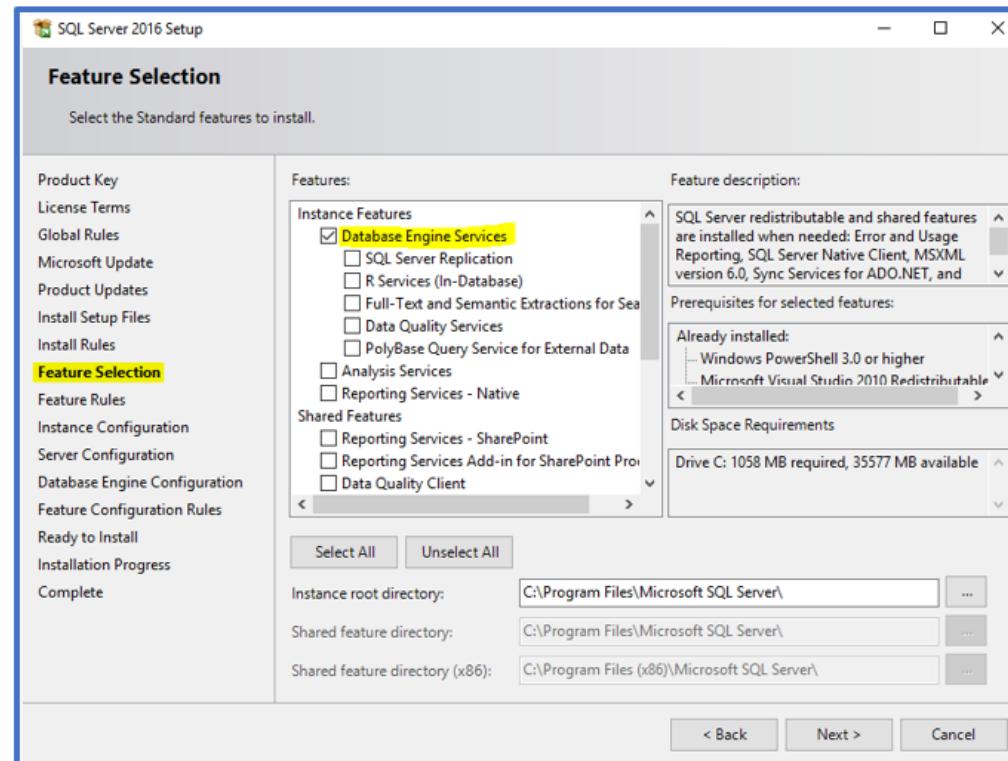
- Confirmation** – Click “Install” (see above). Close out of the Wizard when installation is complete.

SQL Server Installation

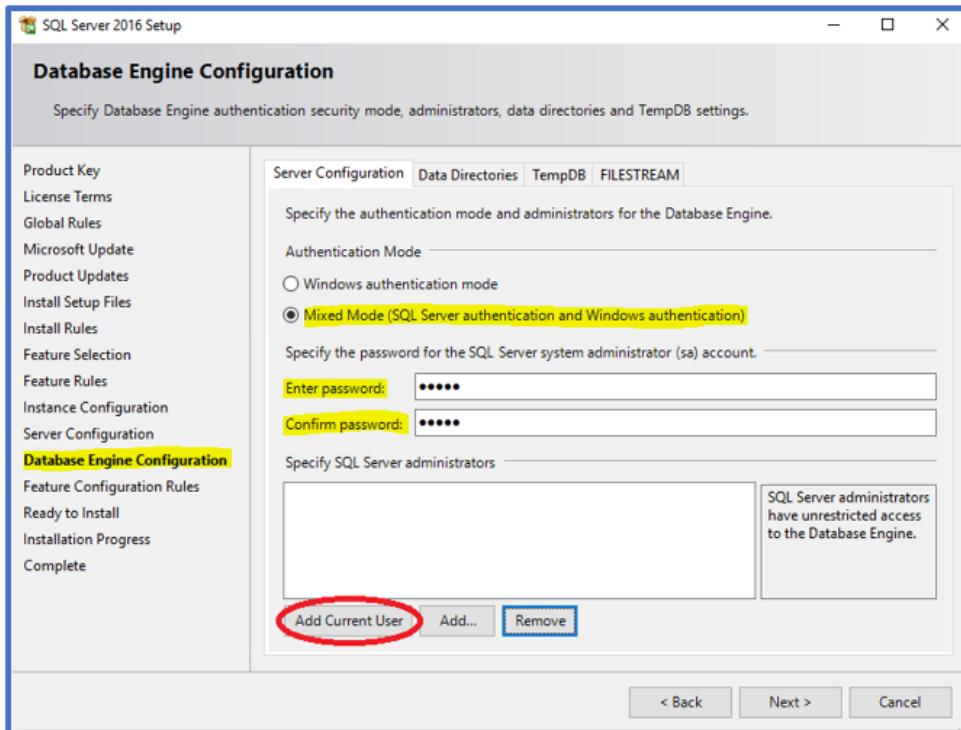
1. To begin the process of installing a new SQL Server on your machine (see below):
 - a. Open Microsoft's "SQL Server Installation Center"
 - b. On the left, select "Installation"
 - c. Click "New SQL Server stand-alone installation"



- d. Input your product key (if needed) and accept the licensing terms to continue the installation.
- e. The defaults for most of the sections will be just fine. However, the two sections you will need to modify are "Feature Selection" and "Database Engine Configuration."



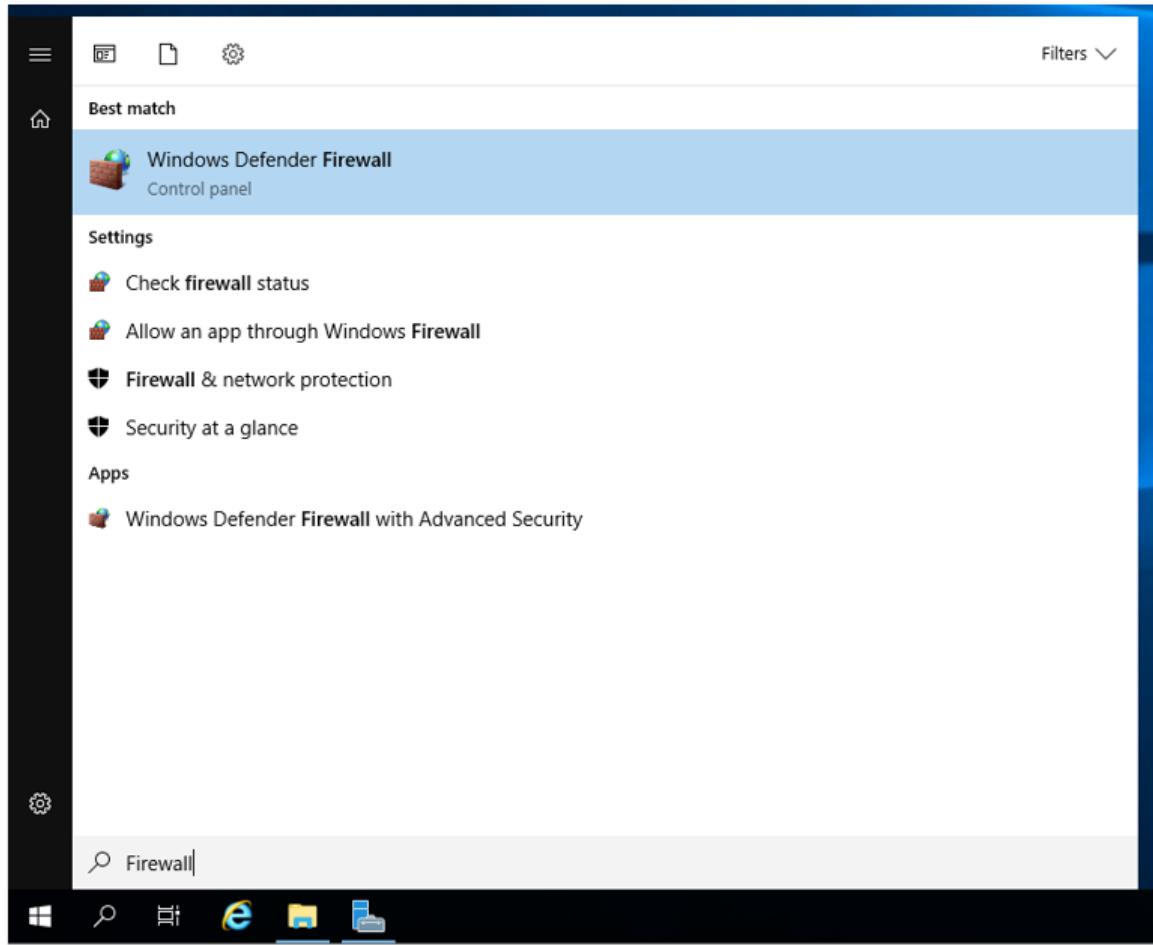
- i. **Feature Selection** (see below) – When you are prompted to select specific server features, check the “Database Engine Services” box and then continue.
- ii. **Database Engine Configuration** (see below) – At the Database Engine Configuration screen, select the “Mixed Mode (SQL Server authentication and Windows authentication)” option.
- iii. Under the same section, you will be asked to create and input a password for the system administrator account. Make sure to remember this information!
- iv. Finally, click the Add Current User button at the bottom. This will populate your current windows account as a user. Once that is complete, click “Next.”



- f. The final step is to click the Install button to finish up this process. Once this is complete, you can close out of the Server Setup window.
- 2. Once your server is up and running, you will need to install the [URL Rewrite Module](#). Simply download the file from Microsoft (see Page 2 links or above hyperlink) and run the application to install the necessary patch.

Firewall Configuration

1. Open Windows Defender Firewall



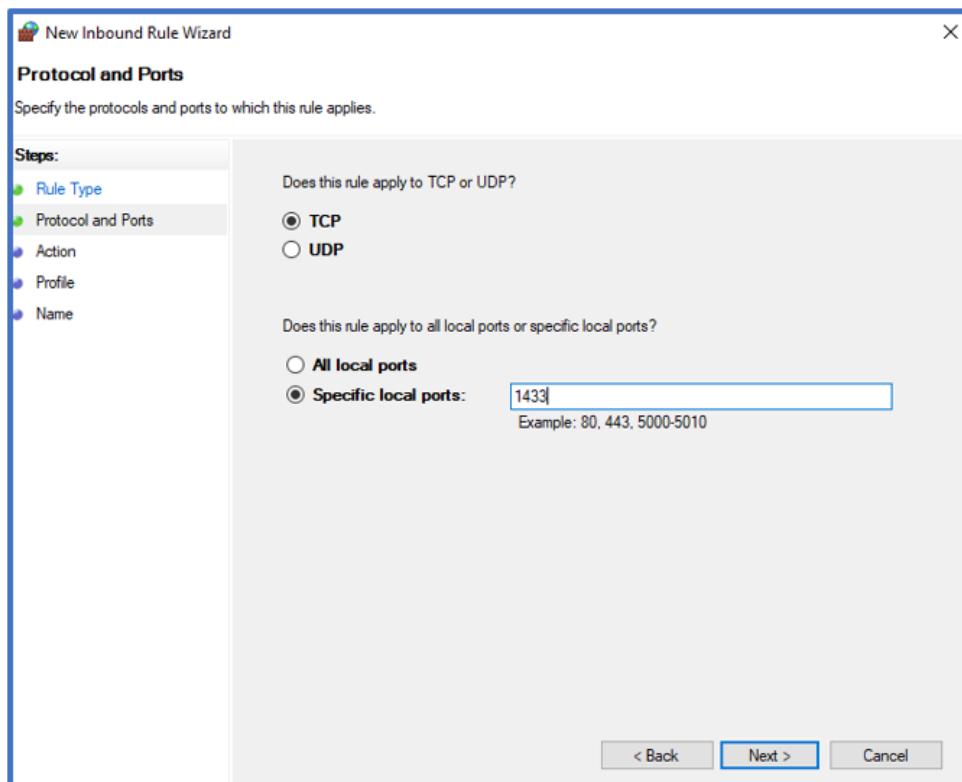
2. On the left, select “Advanced Settings.”

a. Inside the new window, double-click “Inbound Rules” and then select “New Rule” on the right (see below).

A screenshot of the "Windows Defender Firewall with Advanced Security" application. The left pane shows a navigation tree with "Inbound Rules" selected. The main area displays a table titled "Inbound Rules" with columns: Name, Group, Profile, and Enabled. The table lists numerous rules, mostly starting with "Core Networking" or "Cast to Device". The right pane is titled "Actions" and contains a list of options: "Inbound Rules" (highlighted), "New Rule...", "Filter by Profile", "Filter by State", "Filter by Group", "View", "Refresh", "Export List...", and "Help".

b. Rule Type – Select “Port” as the new rule type and click “Next.”

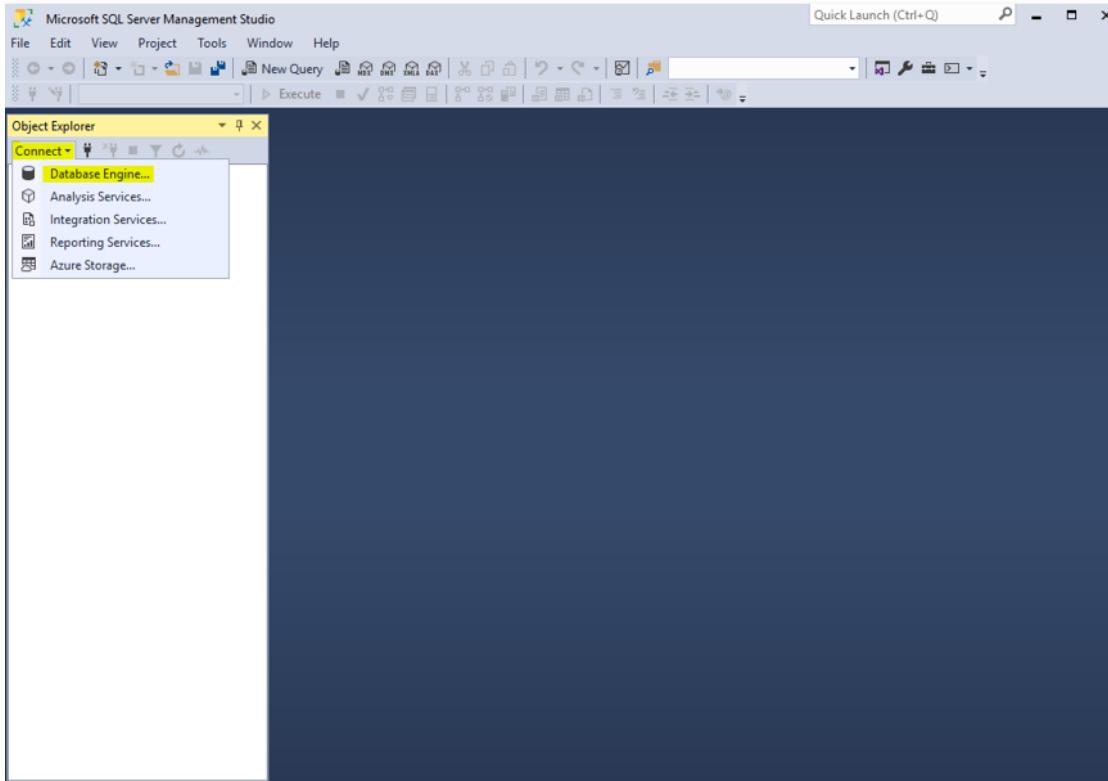
- c. **Protocol and Ports** (see below) – Change the rule to apply to “Specific local ports” and enter your desired port. Once that is finished, click “Next.”



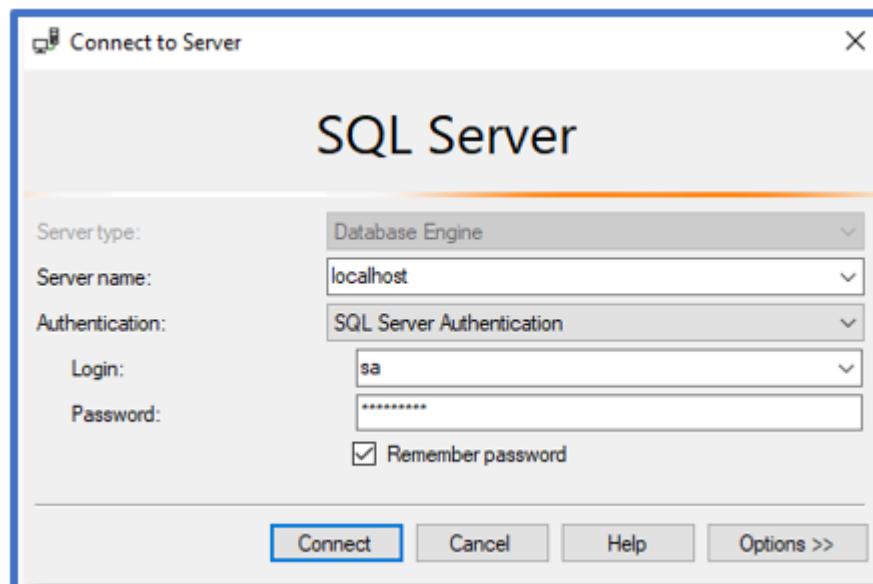
- d. **Action** – Select the “Allow the connection” radio button. This should be selected by default. Click “Next.”
e. **Profile** – Choose what type of networks you wish to allow connections from. If you are unsure, leave them all checked. Click “Next.”
f. **Name** – The final step is to create a name and description for this new rule. Once you’ve done this, click “Finish.”

Database Setup

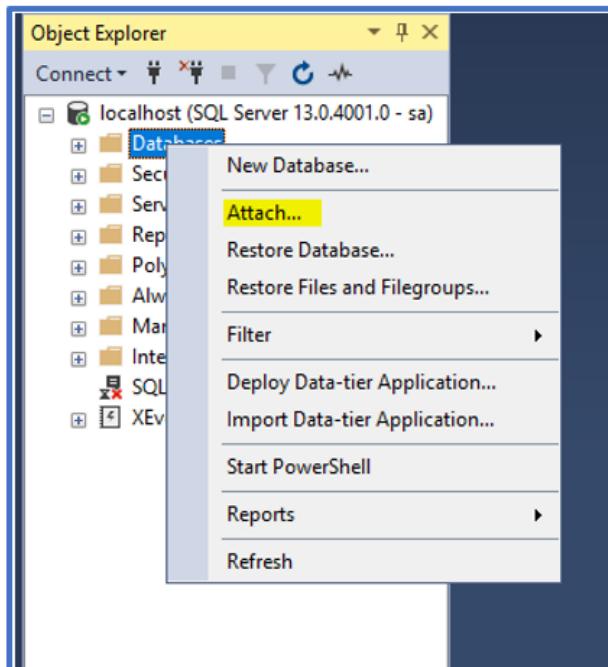
1. Open the CSET 9.2.2 folder that you downloaded earlier and navigate to the “Website” subfolder. Inside this folder you will find another subfolder titled “Data.” Inside the Data subfolder will be two files called “CSETWeb” and “CSETWeb_log.” Copy these two files to your server.
2. Open Microsoft SQL Server Management Studio (see below) and connect to the SQL Server that we setup previously.
 - a. Open the “Connect to Server” dialog box.



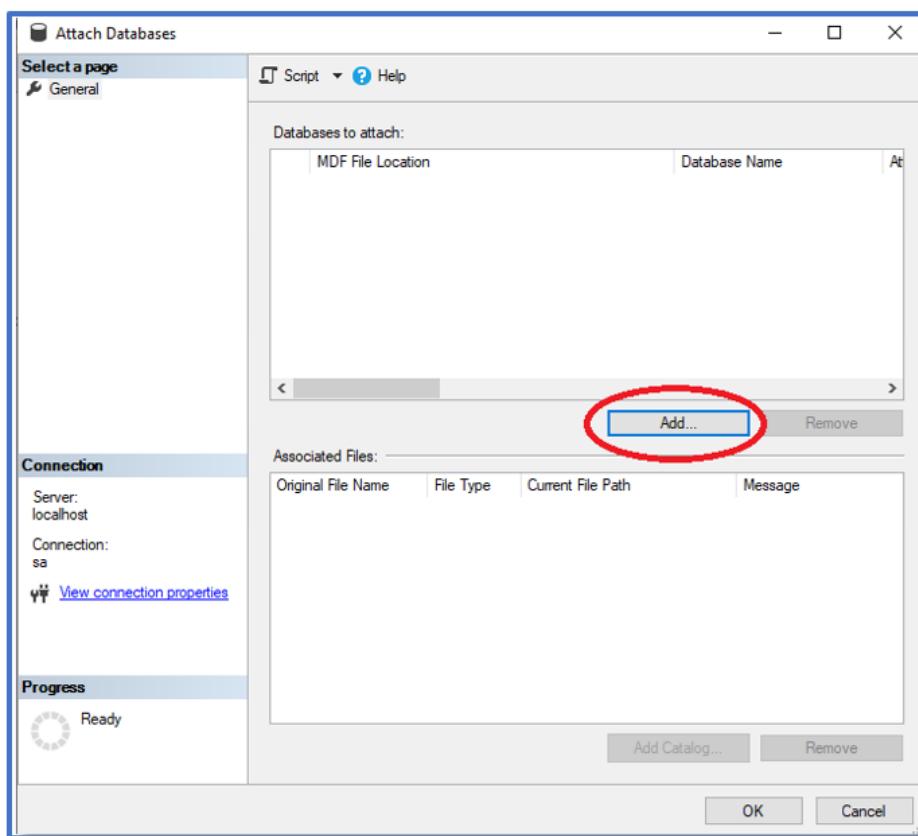
- b. Change the server name to “localhost” or whatever name you have specified for your server already.
- c. Your Server can be run through either the “SQL Server Authentication,” which will require the login information you created earlier, or you can use the Windows Authentication, which will not require any login information as the server will verify your identity through your Windows account.



3. Inside the Object Explorer on the left, right-click the Database folder (see below) and then click “Attach.”



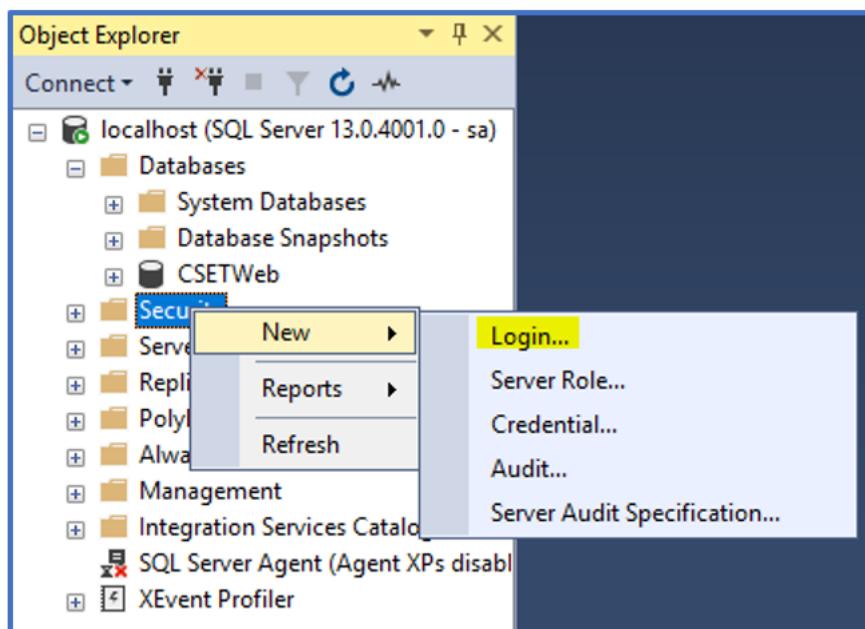
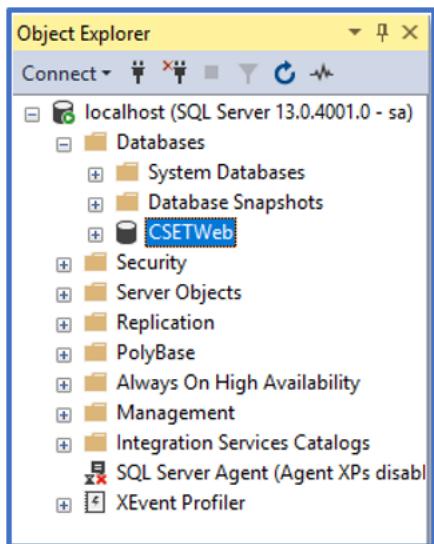
- a. This will bring up the “Attach Databases” dialog box (see below). Click the Add button and navigate to the location where you previously saved/copied the CSETWeb.mdf file. Click on the file and then click “OK,” and then click “OK” again to attach the database.



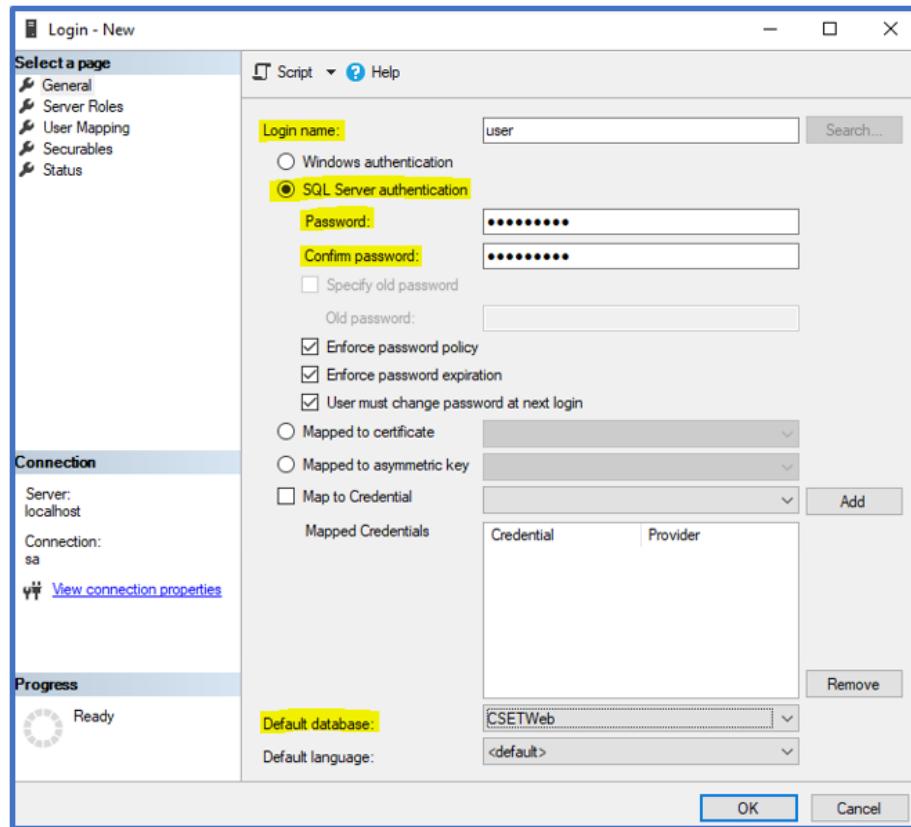
- b. You'll know you've completed this step successfully when you can see the "CSETWeb" object appear under the Databased section in the Object explorer.

Create Database User

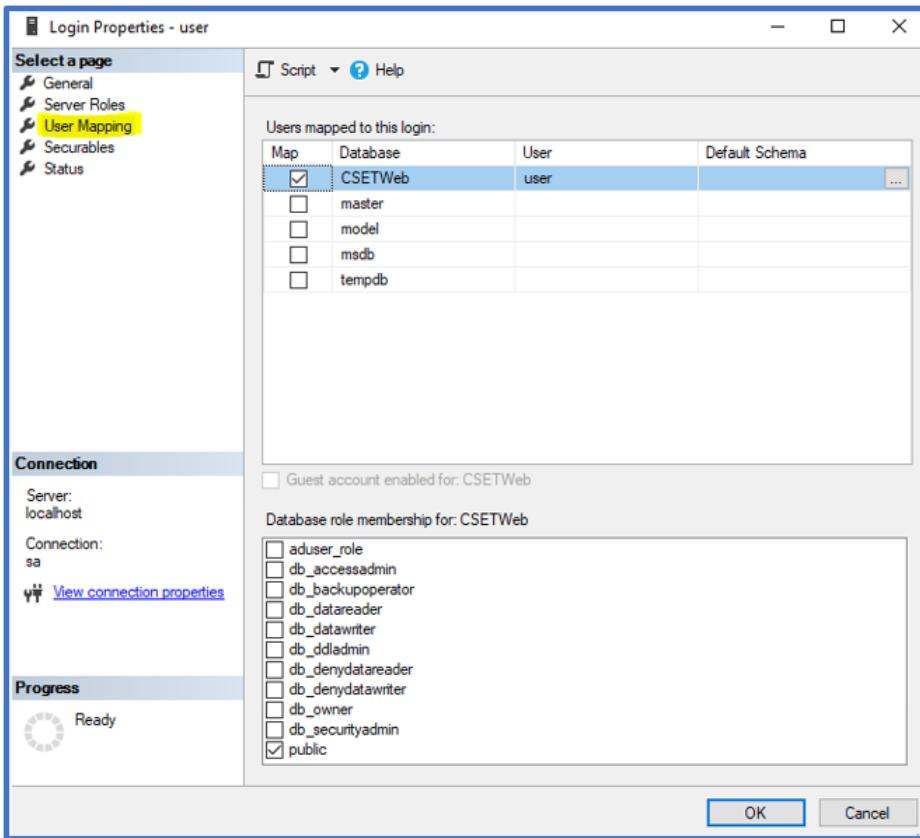
1. Previously we created our SQL Server account. We will now need to create an account that has access to the database. Continuing in the Object Explorer (at right), right-click on the folder named Security, hover over New (below) and then click “Login.”



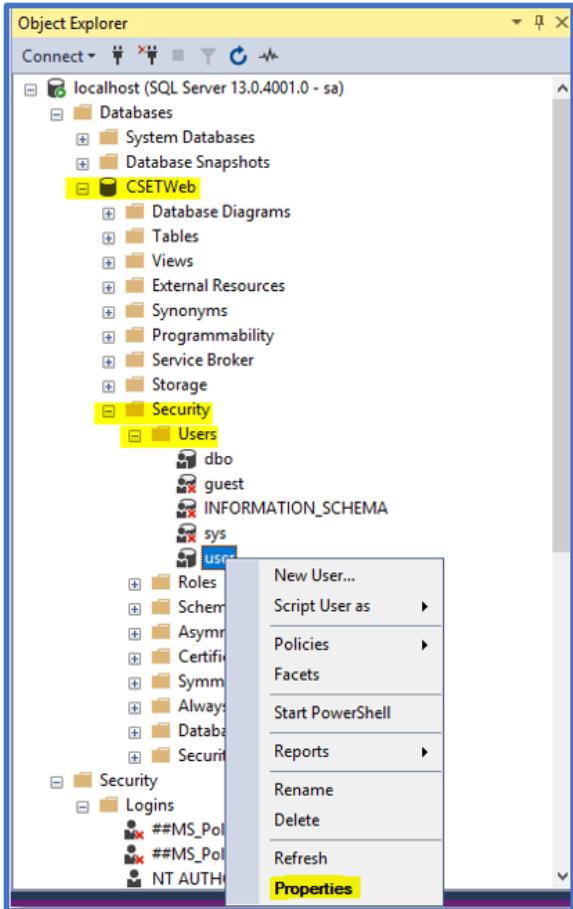
- a. As seen in the below window, enter a login name, select the “SQL Server authentication” radio button, and then enter a password. If you choose to go through the Windows authentication, you will not need to enter a password.
- b. At the bottom of the box, change the Default database to CSETWeb.



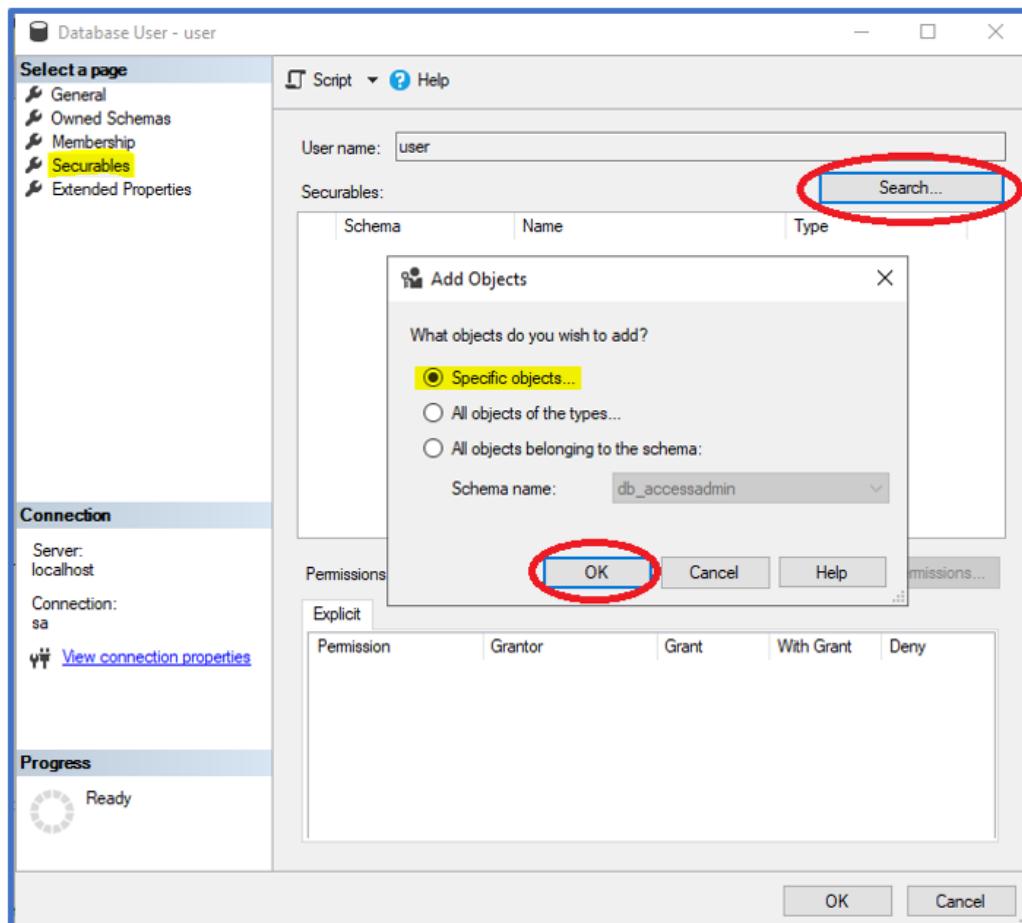
- c. At top-left from the window shown below, click “User Mapping” and then select the CSETWeb checkbox. Then click “OK.”



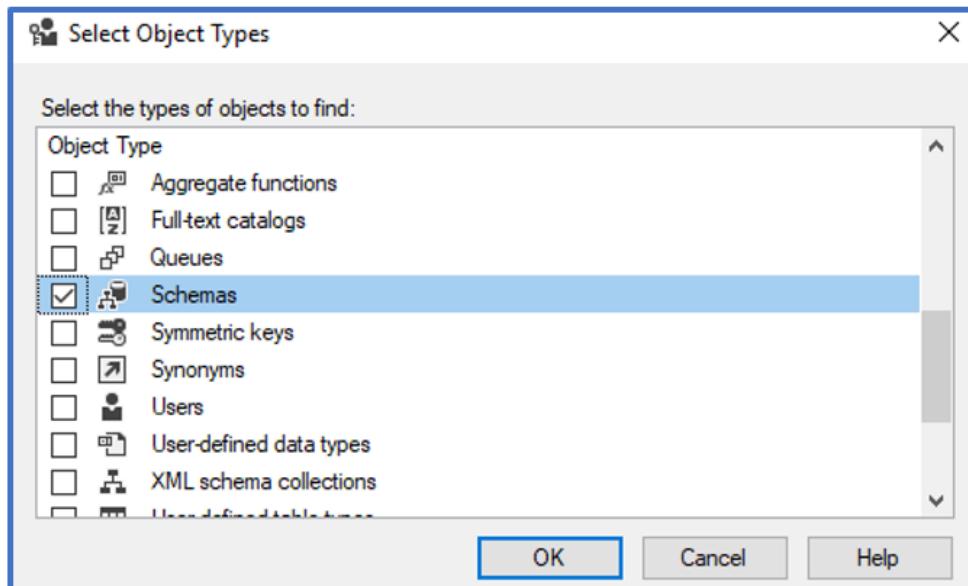
2. Back in the Object Explorer of SSMS (see right), expand the CSETWeb list, followed by Security and then Users. You should see the new user you created listed here. For us, it's simply “user”. Right-click on your user’s name and select properties.



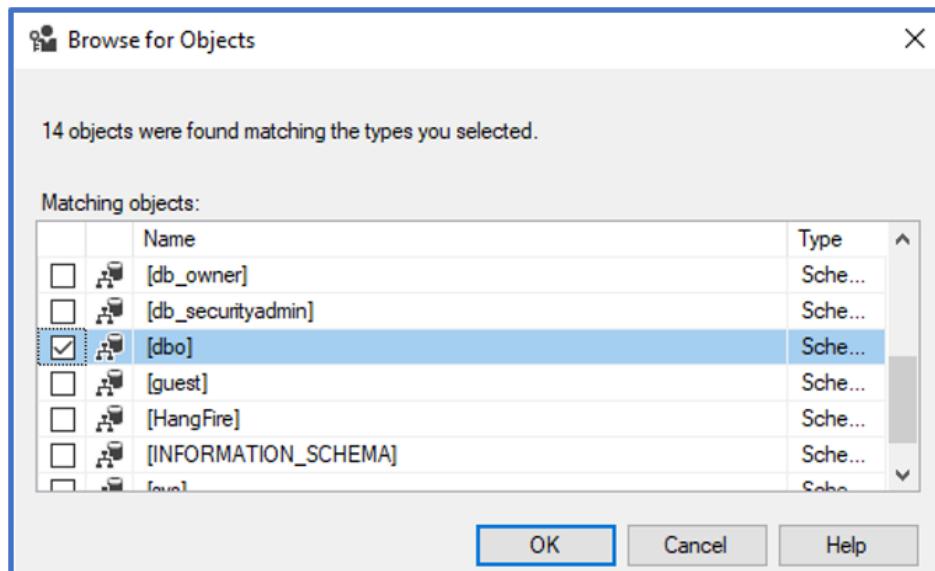
- a. In the dialog box that pops up (see below), select “Securables” from the menu on the left if it is not already selected.
- b. Click the Search button to generate another dialog box. Make sure the “Specific objects...” radio button is selected and then click “OK.”



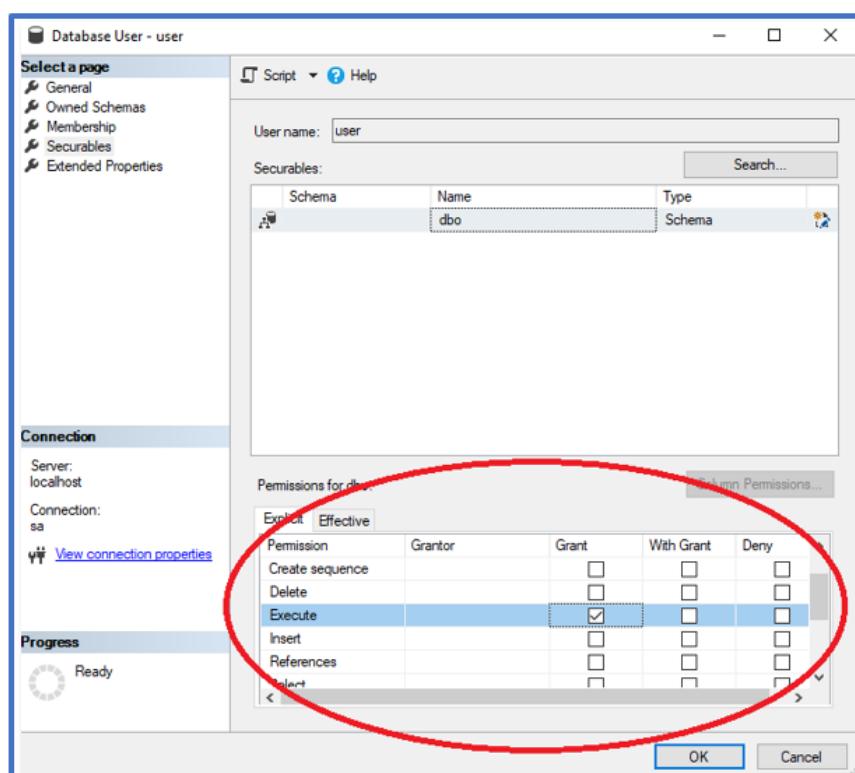
- c. Once you hit OK, you should see yet another box pop-up titled “Select Object.” Click the button that says Object Types... This will generate a list of object types. Scroll down until you see the “Schemas” object (see below). Check this box, and then click “OK.”



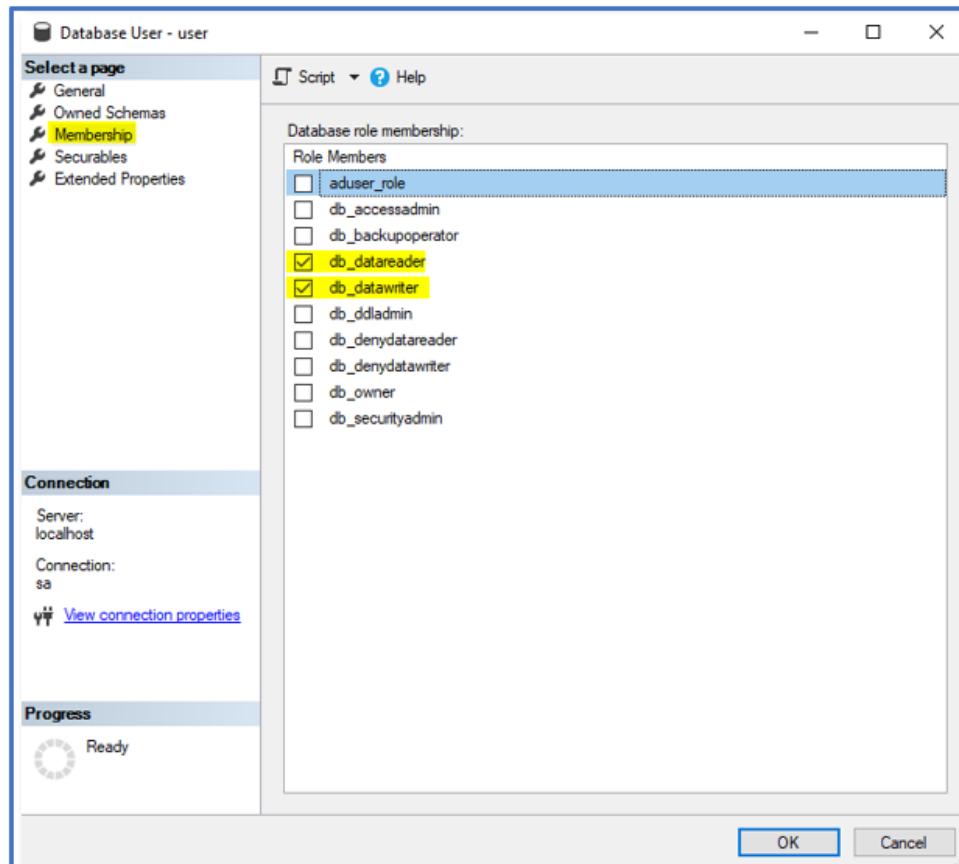
- d. Next, click “Browse” and select the [dbo] checkbox. Then click “OK.”



- e. Once we have our dbo inside our Securables, we need to grant it permissions. Scroll through the list of permissions and when you find the “Execute” permission, select the Grant checkbox.

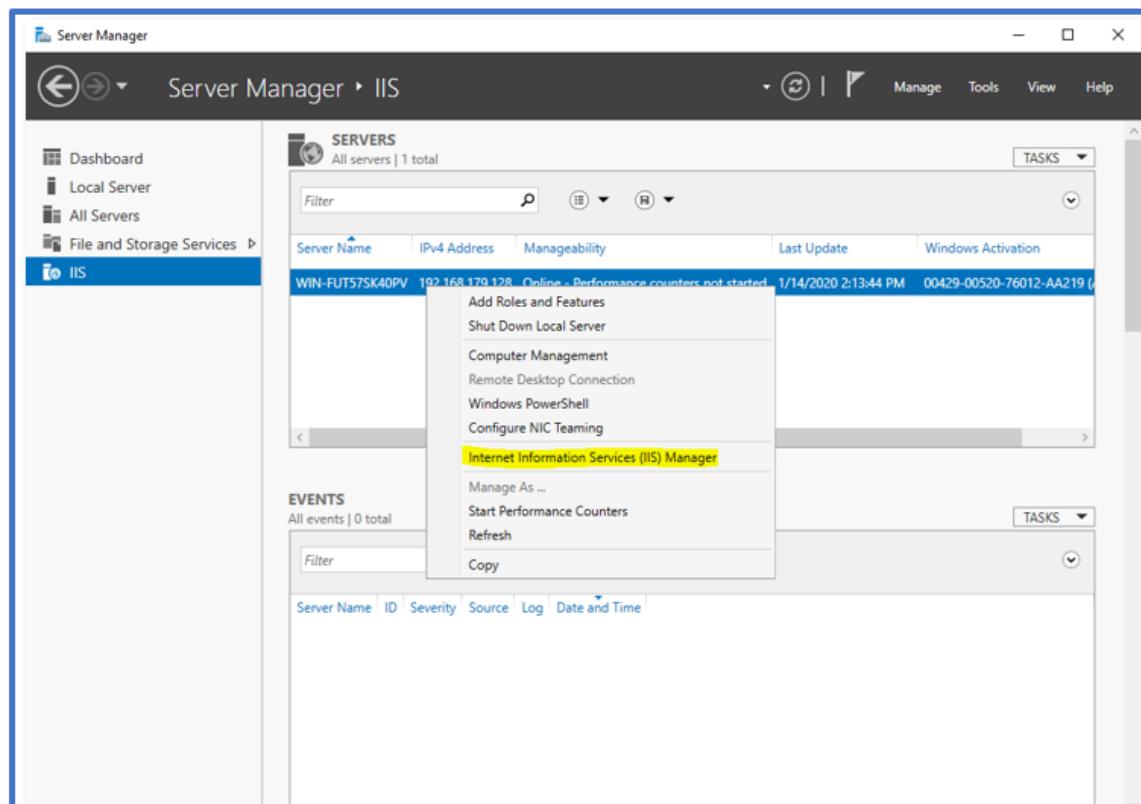


- f. Our final step is to go over to the Membership page (see below) and select the checkboxes for “db_datareader” and “db_datawriter.” Then select “OK.”

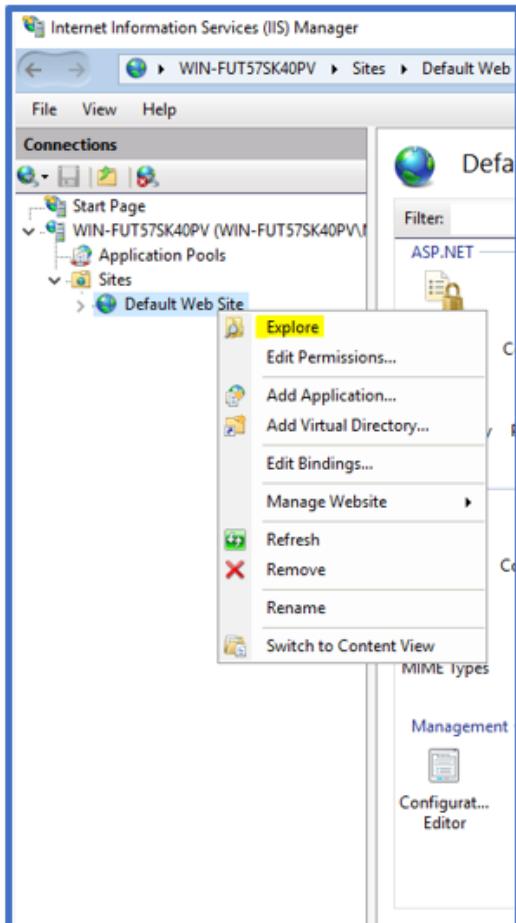


CSET Installation

1. Re-open Windows Server Manager (see below). Double-click on “IIS” on the left. Then, right-click on the server name and click “Internet Information Services (IIS) Manager.”

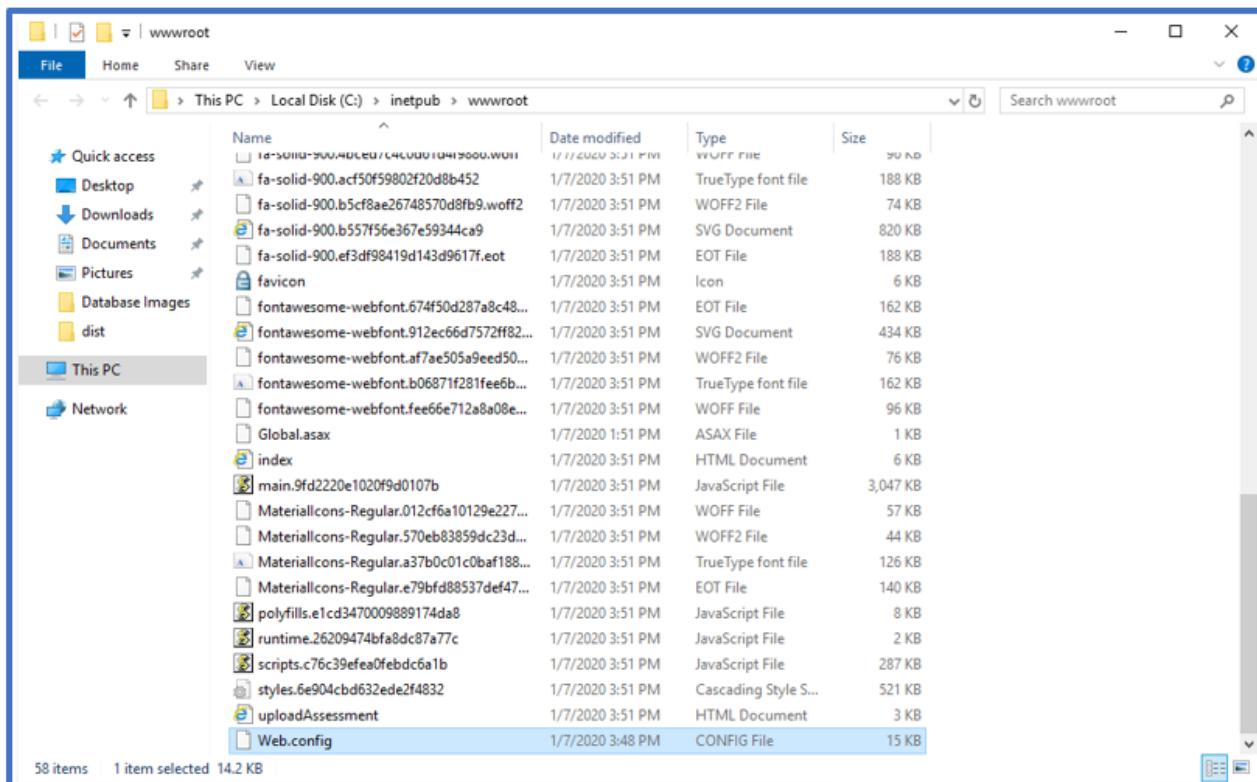


- a. As seen in the window at right, expand the server's name drop-down list and then expand the Sites drop down list. You should see a "Default Web Site" item. Right-click this item and select "Explore". This will open the "wwwroot" folder.
- b. Delete everything inside this folder **EXCEPT** for the "aspnet_client subfolder".
 - i. If you've done any kind of changes or work inside this folder previously, we recommend copying the contents to preserve those changes as deleting the files will erase any changes you have made.
- c. From the CSET 9.2.2 folder, copy all the contents and files of the Website subfolder into your wwwroot folder.



CSET Configuration

1. Locate and open a file called "Web.config" inside the "wwwroot" folder. Open this file using a text editor such as notepad.



- Scroll to the bottom of the document and you will find the <connectionStrings> section. We will need to edit these to correctly connect to CSET.
- On each of the lines inside the two connection string tags, there is a part that says “data source=...” You will need to change the part *after* the equals sign to the IP address or domain name of the machine on which the SQL Server is running.

```
<connectionStrings>
  <add name="CSET_DB" connectionString="data source=localhost;initial catalog=CSETWeb;persist security info=True;Integ
  <add name="ElmahConn" connectionString="data source=localhost;initial catalog=CSETWeb;persist security info=True;Ini
  <add name="HangfireConn" connectionString="data source=localhost;initial catalog=CSETWeb;persist security info=True;
</connectionStrings>
```

- If IIS and the SQL Server instance are running on the same machine, you can use “localhost” as the domain name. Otherwise, you will need the specific domain or IP address to connect properly.
- On each of the same lines, you will need to update the “Integrated Security=SSPI” section to reflect your SQL Server specific login info.

```
<persist security info=True;user id=user;password=AbC!2#;Multi
';persist security info=True;user id=user;password=AbC!2#;Mul
Web;persist security info=True;user id=user;password=AbC!2#;I
```

- If you are using the Windows domain authentication method, then you will use “Trusted_Connection=SSPI” instead of a user ID and password.
- Save and close the Web.config file.
 - If you receive an error stating that you do not have permissions to save the Web.config file, find the file inside the wwwroot folder and right-click on it. Select properties and go into the security tab. Click on the edit button and make sure that all users have “Full Control” over the file.
- Go back to the “Internet Information Services (IIS) Manager” and on the right, make sure the server is running. You may now browse to your Enterprise CSET Installation.

Other Steps (Optional)

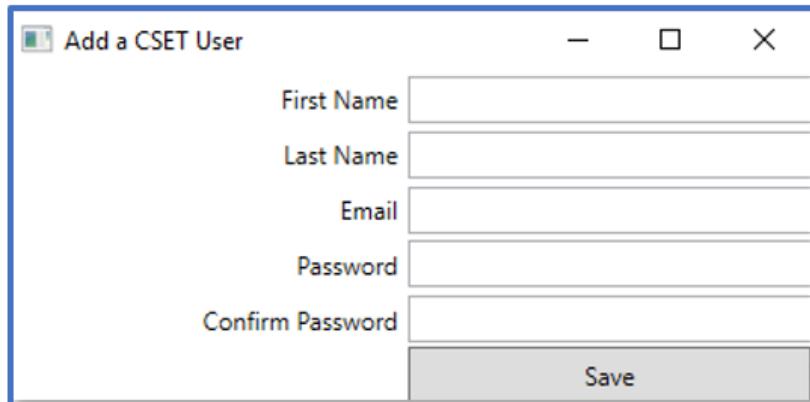
Creating a CSET User:

There are two ways to add a new user to your freshly created CSET Stand-Alone. The first way is to register for a new account inside the CSET application itself. This will require a valid mail host as user's will be required to enter their email address and receive a confirmation email on your network.

1. Using a browser, navigate to your CSET webpage.
2. At right, select "Register New User Account."
3. Enter your information (name, email, and security questions), and select "Register."
4. A confirmation email will be sent to the email you entered. This email will contain a temporary password that will allow you to login to the CSET Application.
5. Once a user has logged in for the first time, they will be prompted to create their own password to replace the temporary one.

The second way to add a new user to your CSET Application is to use the included "AddUser" program. This tool is intended more for testing purposes than company-wide use. It allows anybody to create a new user without the email check and should only be used by administrators. As such, do not place this program in a public or shared folder on your system.

1. Inside the "AddUser" folder, you will find a file called "AddCSETUser.exe". It's a config file. Open this file with a text editor such as notepad.
 - a. Inside the <connectionStrings> tags, you will need to change your "data source=" to the IP Address or domain of your server.
 - b. You will then need to change the "user id=" and "password=" to the admin account you created previously.
 - c. Save and close the file.
2. Double-click on the "AddCSETUser" application and a small dialog box should pop-up with entry fields to add a new CSET User.



- a. Enter the required information and click "Save."
- b. If you've connected with the server properly, you will see small green text at the bottom-left of the box that says, "Added Successfully". You may now login to CSET® using that user account.

Mail Host Setup:

1. Inside your "wwwroot", open the Web.config file.
 - a. Inside the config file, you will need to locate the "SMTP Host", and "Sender Email" portions.

```
<appSettings>
  <add key="webpages:Version" value="3.0.0.0" />
  <add key="webpages:Enabled" value="false" />
  <add key="ClientValidationEnabled" value="true" />
  <add key="UnobtrusiveJavaScriptEnabled" value="true" />
  <add key="JWT Expiry Minutes" value="60" />
  <add key="CORS Allowed Origin" value="*" />
  <!-- Email settings -->
  <add key="SMTP Host" value="mailhost.inl.gov" />
  <add key="SMTP Port" value="25" />
  <add key="Sender Email" value="no-reply@example.com" />
  <add key="Sender Display Name" value="CSET User Administration" />
  <add key="DEBUG EMAIL RECIPIENT_____ " value="" />
  <add key="Allow Test Email" value="true" />
  <!-- COMMENT OUT IN PRODUCTION -->
</appSettings>
```

- b. Edit the text after the equal sign of value to your domain name. (e.g. value="mailhost.YOURDOMAIN.com").
- c. Save and close the file when you are finished.

Adding an SSL Security Certificate for Extra Security:

An SSL certificate is a web technology that establishes a secure link between a web server and a browser. This link encrypts all data (such as passwords) so that your server is more secure.

1. You can follow this tutorial: <https://www.digicert.com/ssl-support/pfx-import-export-iis-7.htm> to add an SSL certificate to your CSET stand-alone.

Evaluation Preparation

Two preliminary tasks are required before using the tool to perform an assessment: (1) forming the subject matter team and (2) collecting the network/architecture documentation and related information.

Subject Matter Team Selection

The first step is to select a cross-functional assessment team consisting of subject matter experts selected from various operational areas in the organization. Organizations may add additional team members as needed to address specific topics. Anyone in the organization who has had training or experience with the CSET tool should be included on the team.

The primary user should spend some time using the CSET tool with test-only or dummy data prior to commencement of the team activity. Familiarity with the CSET tool will improve speed and ease of use.

Representatives from the following areas are suggested for an effective assessment. The representatives should have significant expertise in their areas of responsibility.

If performing an ICS assessment:

- Industrial Control Systems (knowledge of industrial control system architecture and operations)
- System Configuration (knowledge of systems management).
- System Operations (knowledge of system operation).

For either an ICS or IT assessment:

- IT Network/Topology (knowledge of IT infrastructure).
- IT Security/Control System Security (knowledge of policies, procedures, and technical implementation).
- Risk Management (knowledge of the organization's risk management processes and procedures).
- Business (knowledge of budgetary issues and insurance postures).
- Management (a senior executive sponsor/decision maker).

Gather Supporting Documentation and Information

Previous CSET users have found that the following types of documents and information are useful to have during completion of the assessment. Collecting this reference information before beginning the assessment is advisable:

- Organizational chart that outlines responsibilities;
- Annual operating and capital budgets;
- Insurance policy description;
- Previously performed risk and vulnerability assessments;
- Capacity, operation, management, and maintenance manuals;
- Risk management documentation;
- Hazardous waste operations and emergency response Standards;
- Emergency Operations Plan/Emergency Response Plan;
- Asset inventory and criticality rating from Computerized Maintenance Management System (CMMS);
- Inventory list of process control/SCADA software and hardware, including interfaces;
- Network topology diagram and supporting documentation;
- Documentation/knowledge from previous incidents or near misses;
- General asset inventory, criticality asset determination, business impact analyses, contingency plans, etc.; and
- Information security policies, plans, and procedures.

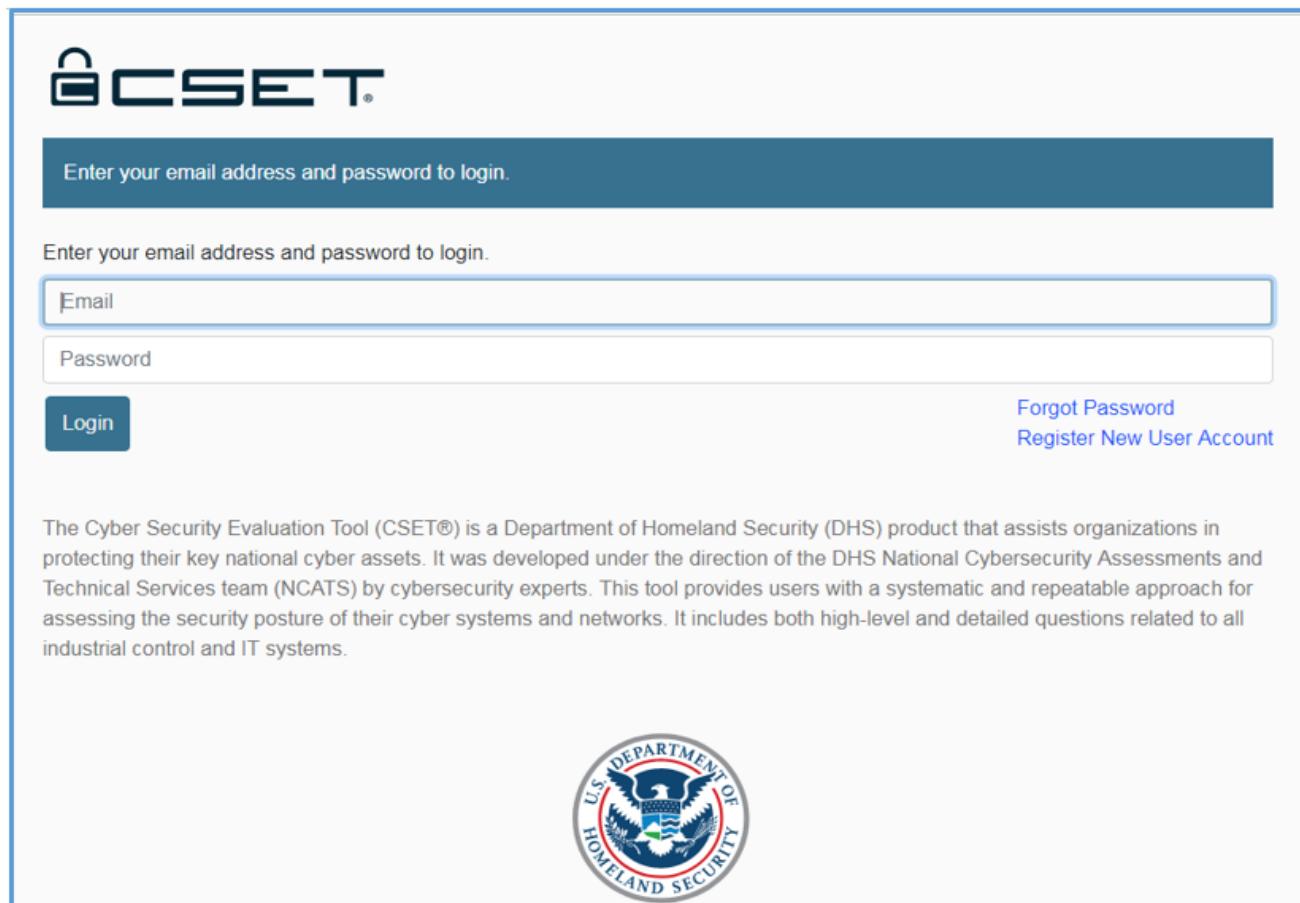
When the assessment team is prepared and supporting documents are gathered, the organization is prepared to start CSET and begin the actual evaluation.

Start CSET

Go to <http://localhost:46000/index.html> or for other installation options the instructions provided in the help section titled [Installation Procedure](#) should be followed.

The actual URL maybe provided by your companies CSET administrator.

The CSET home screen will be displayed as seen in the figure below.



The screenshot shows the CSET login page. At the top, there is a logo consisting of a lock icon followed by the text "CSET®". Below the logo, a blue header bar contains the text "Enter your email address and password to login.". The main content area has a light gray background and contains the following elements:

- A text input field labeled "Email".
- A text input field labeled "Password".
- A blue "Login" button.
- Links for "Forgot Password" and "Register New User Account" in blue text.

At the bottom of the page, there is a circular seal of the U.S. Department of Homeland Security. The seal features an eagle with wings spread, perched on a shield with stars and stripes. The words "U.S. DEPARTMENT OF HOMELAND SECURITY" are inscribed around the eagle.

Figure: CSET home screen

Register a User Account

To get started in CSET you must have a registered account.

First, select the "Register New User Account" link. The Register Account dialogue will open.

The screenshot shows the CSET home page. At the top, there is a logo and a header bar with the text "Enter your email address and password to login.". Below this, there is a form for logging in with fields for "Email" and "Password" and a "Login" button. To the right of the login form, there are two links: "Forgot Password" and "Register New User Account". A red dashed box highlights the "Forgot Password" and "Register New User Account" links. Callouts numbered 1 through 4 point to specific elements: 1 points to the "Forgot Password" link, 2 points to the "Login" button, 3 points to the "Forgot Password" link, and 4 points to the "Register New User Account" link. Below the login form, there is a brief description of what CSET is and the Department of Homeland Security seal.

Figure: Using the home screen to register an account

The screenshot shows the CSET registration dialogue. It starts with a header bar that says "Enter your name and email address to register a new CSET account.". Below this, there are four text input fields: "First Name *", "Last Name *", "Email *", and "Confirm Email *". After these fields, there is a note about security questions: "Providing security questions is optional but will allow you to recover your password should you forget it." Below this note, there are two sections: "Security Question" and "Security Answer". The "Security Question" section contains a dropdown menu with options like "What was the house number and street name you lived in as a child?". The "Security Answer" section contains two text input fields with the placeholder "Answer". At the bottom left is a "Register" button, and at the bottom right are links for "Login" and "Forgot Password".

Figure: Registration dialogue

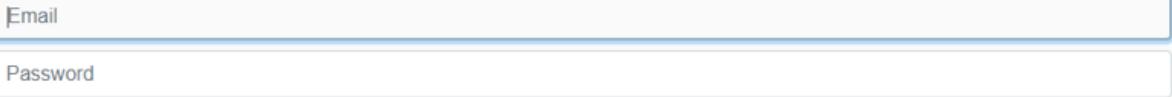
The user should enter their first and last name and email.

Users have the option to add security questions next. They are not required but will be another step in ensuring their identity when resetting a password. Users can select a question from the dropdown or create a custom question.

Select the "Register" button. The user will be sent an email with a temporary password and instructions to login. Users can navigate to CSET through the email or select the "Login" link on the dialogue above.

Warning: Users CAN NOT register an email that has already been registered.

1 Login Email and Password fields



The image shows a screenshot of a login interface. It consists of two input fields: one labeled 'Email' and another labeled 'Password'. Both fields are empty and have a light blue border.

To login enter the user's email and password here.

2 Login button



Click the login button after entering user information to login.

3 Forgot Password link

[Forgot Password](#)

This link opens a dialogue for user's to get a new temporary password and reset their old forgotten password.

4 Register Account link

[Register New User Account](#)

This link will open a dialogue for the user to create a new account.

Import/Export a CSET Assessment

There are two different ways to import a CSET assessment.

Pick an option below to learn more.

Importing a .csetw File

With the web-based version of CSET you can import a .csetw file. To begin click the Import button to begin the process.

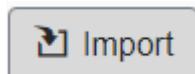


Figure: Import Button

The file explorer will open, and at this point you can select a .csetw file. A new assessment that is a duplicate of the uploaded assessment will show in the landing page.

NOTE: The web-based version of CSET only supports .csetw file upload. For legacy file (.cset) upload the user must use the stand-alone install.

Importing a .cset File

With the stand-alone version of CSET running locally you can import a legacy CSET file.



Much like importing a .csetw file click the **Import** button on the local Landing page.

The file explorer will open. Select the .cset file to import. The upload dialogue will open. Once the dialogue has closed, refresh the landing page to see the imported assessment.

Exporting a CSET Assessment

To export an assessment simply select the Export button next to the assessment to be exported on the Landing page.

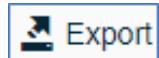


Figure: Export button

After clicking the Export button the assessment will be downloaded as a .csetw file and will be in the user's Downloads folder (unless otherwise specified in browser settings).

Title Bar

The Title Bar allows the user to access high-level functions of the CSET application and is shown in the figure below.

The screenshot shows the CSET application interface with the following elements highlighted:

- CSET Home** (1) - The main navigation button.
- Tools** (2) - A dropdown menu button.
- Resource Library** (3) - Another dropdown menu button.
- Help** (4) - A dropdown menu button.
- User Profile** (5) - The user's account information.

The main content area displays "My Assessments" with a table:

Assessment Name	Last Modified	Primary Assessor	Status
Test 1	27-Aug-2019	Your Username	Remove Export
(Untitled Assessment)	27-Aug-2019	Your Username	Remove Export
Test 3	27-Aug-2019	Your Username	Remove Export
(Untitled Assessment)	29-Aug-2019	Your Username	Remove Export

A large watermark of the "HOMELAND SECURITY" seal is visible in the background of the content area.

Figure: Title Bar

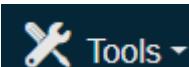
1 CSET Home



The CSET HOME button opens the user's landing page.

For more information about the landing page, see the [Landing Page](#) help section.

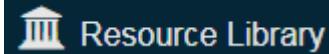
2 Tools



The Tools button opens the Tools menu.

For more information about the Tools menu, see the [Tools Menu](#) help section.

3 Resource Library



The Resource Library button opens the Resource Library.

For more information about the Tools menu, see the [Resource Library](#) help section.

4 Help



The Help button opens the Help menu.

For more information about the Help menu, see the [Help Menu](#) section.

5 User Profile



Your Username ▾ (This will display your user name)

The User Profile button opens the User Profile menu.

For more information about the User Profile menu, see the [User Profile](#) help section.

Tools Menu

The Tools Menu provides the user with options outside of the assessment process. The user can access the Enable Protected Features, Assessment Documents, Parameter Editor, Export Assessment to Excel, Import Modules, and Module Builder. The Tools Menu is described in the figure below.

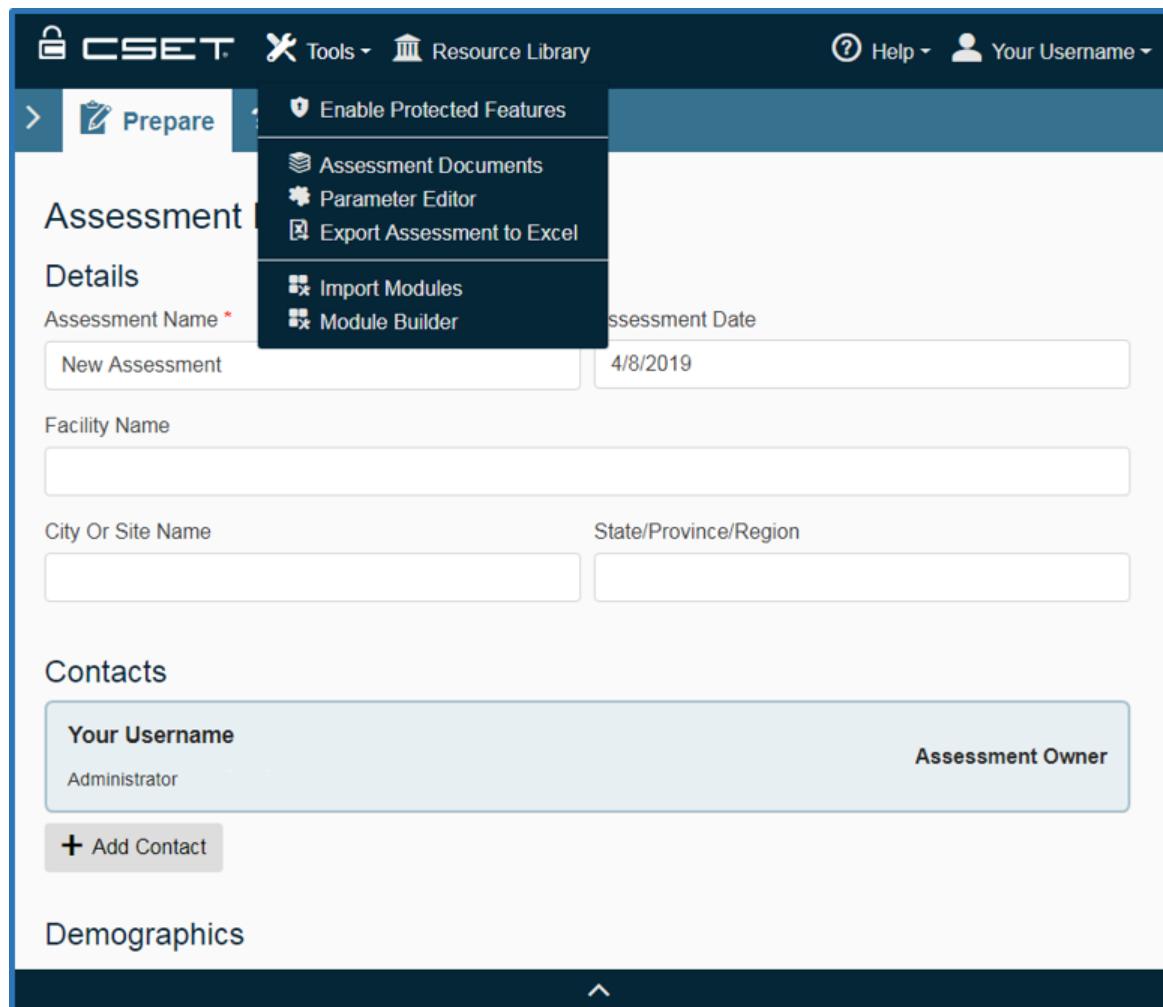


Figure: Tools menu



Click the Tools menu button  to open the Tools menu.

Enable Protected Features: Clicking the Enable Protected Features menu item displays the Protected Features window that allows the user to view specific questionnaires or standards developed by specific industries that are not available to the general public.

See [Protected Features](#) for more information.

Assessment Documents: Clicking the Assessment Documents menu item opens the Assessment Documents window that allows users to review documents that have been assigned to specific questions of the assessment. If there are no documents associated with the assessment the list will return blank.

See [Assessment Documents](#) for more information.

Parameter Editor: Clicking the Parameter Editor menu item displays the Parameter Editor window where users can maintain parameters related to their selected Standard in requirements mode, if they are supported.

See [Parameter Editor](#) more information.

Export to Excel: Clicking the Export to Excel menu item downloads an excel spreadsheet with the answers to the assessment Questions or Requirements.

See [Export to Excel](#) for more information.

Import Module: The Import Modules menu item holds the Import Module feature used for custom standard import.

See [Import Module](#) for more information.

Module Builder: Clicking the Module Builder menu item opens the Module Builder feature that users can build new question and requirements sets.

See [Module Builder](#) for more information.

NOTE: The Assessment Documents, Parameter Editor, and Export to Excel features are not available unless within an assessment. If on the landing page the Tools menu will look like the figure below.

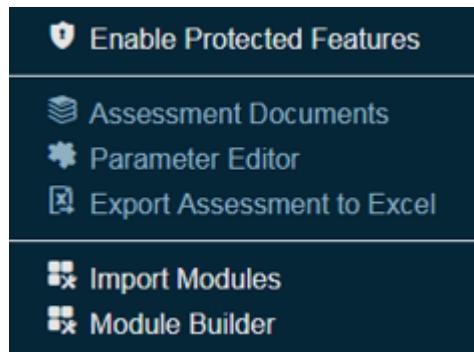


Figure: Tools menu outside of an assessment

Assessment Documents

This section contains information on the purpose and use of CSET Assessment Documents. The Assessment Documents window stores documents and files added to the assessment by the user. These files are associated with specific questions to help explain or to provide evidence for the answer given.

The Assessments Document window provides a way to see all the files that have been stored in the assessment by the user. During the assessment, a document can be added using the Add Document button in the documents section of the Question Details panel that will associate the document with that question. The Assessment Documents is accessed from the Tools menu.

The [Documents](#) help section provides more detailed information on how to associate documents with a question.

Clicking the Assessment Documents menu item in the Tools Menu displays the Assessment Documents window seen in the figure below.

View or download assessment documents via the dialogue.

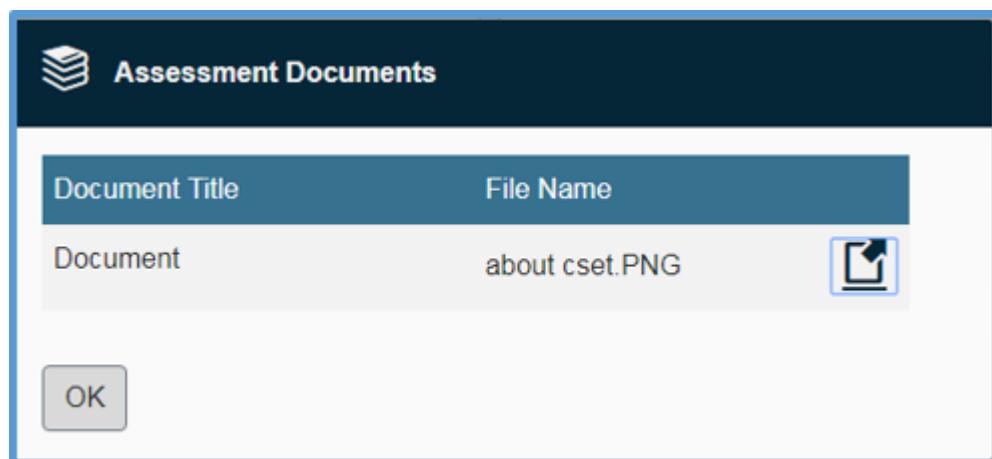


Figure: Assessment Documents window

Parameter Editor

Many Cybersecurity Standards in CSET contain parameter information in the requirement text. Parameters are indicated by [] symbols in the requirement text. For example, the SP800-53 R4 App J Standard contains the following parameter: [Assignment: organization-defined frequency, at least annually].

The Default Parameter Editor allows the user to replace the default parameter text with other text the user defines. So in the previous example, the user might replace the [Assignment: organization-defined frequency, at least annually] parameter with the word Annually. The Default Parameter Editor will then replace all occurrences of the parameter with the user's text.

Users can also change the parameters within the Requirement text itself with inline parameter editing. Simply click in to the parameter edit and save.

The Default Parameter Editor window is described in the figure below.

The screenshot shows the 'Parameter Editor' window with a dark header bar containing a gear icon and the title 'Parameter Editor'. Below the header is a descriptive text block: 'Many Standards in 'Requirements Mode' contain parameters that you can change to match your specific situation. The table below allows you to change the parameter values for the indicated parameter names in this Assessment by clicking on the Default Parameter Value. Changing a default parameter value will update all related parameter values in the requirement text of the currently selected Cybersecurity Standard(s).' A table follows, with columns 'Parameter Name' and 'Default Parameter Value'. The table rows are:

Parameter Name	Default Parameter Value
[Assignment: organization-defined time period]	[Assignment: organization-defined time period]
[Assignment: organization-defined frequency]	[Assignment: organization-defined frequency]
[Assignment: organization-defined types of digital and non-digital media]	[Assignment: organization-defined types of digital and non-digital media]
[Assignment: organization-defined security measures]	[Assignment: organization-defined security measures]
[Assignment: organization-defined list of information system components]	[Assignment: organization-defined list of information system components]

At the bottom left is an 'OK' button.

Figure: Default Parameter Editor window

Parameter List: The Parameter List displays a list of Parameter Names and associated Default Parameter Values.

The Parameter Name column shows the name of the parameter and cannot be changed.

The Default Parameter Value column displays the current parameter values associated with the parameter names for the selected Standards as seen in the Requirement text on the Assessment screen. The parameter values are initially the same as the Parameter Name but can be changed by the user. To change a parameter value, double-click the cell containing the desired Default Parameter Value and enter new parameter text. Perform the same with any other parameters. Once finished, click the "Ok" button.

All parameter values in the requirement text will then be updated with the entered text for the given parameter names throughout the assessment.

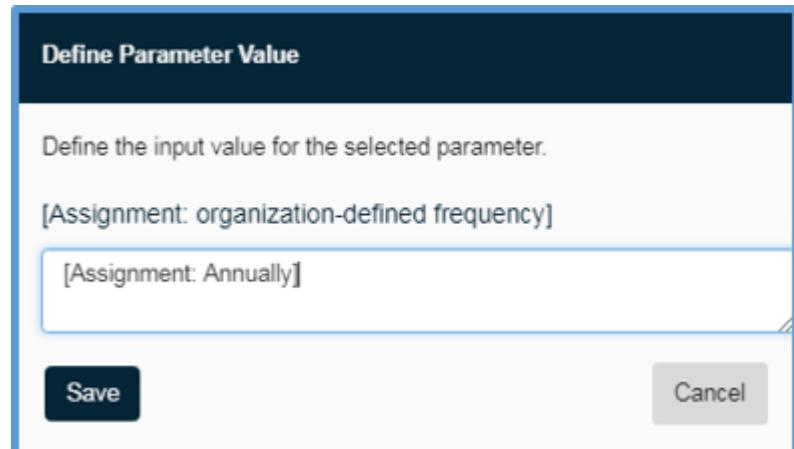


Figure: Inline Parameter editor

Protected Features

The Protected Features window allows the user to add a feature unlock code to release specific standards or questionnaires that are not available to the general public. The Protected Features window is described in the figure below.

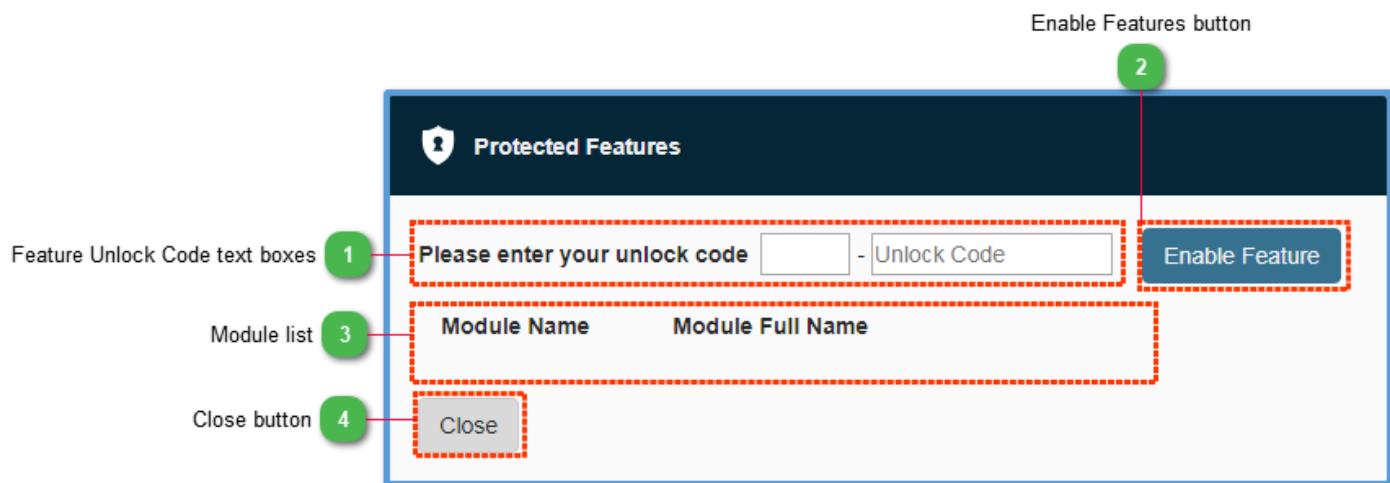


Figure: Protected Features window

1 Feature Unlock Code text boxes

Please enter your unlock code - Unlock Code

The Feature Unlock Code input text boxes allow the user to enter the feature unlock code. Once a proper code has been entered, the Module List will display all available standards or questionnaires that can be added to the CSET Standards Selection screen.

2 Enable Features button

Enable Feature

Select the Enable Feature button after entering the Unlock Code.

3 Module list

Module Name	Module Full Name
-------------	------------------

The Module List displays a list of available standards or questionnaire modules that are unlocked and available in the Cybersecurity Standards Selection page.

4 Close button

Close

The Close button closes the Protected Features dialogue and commits changes.

Export to Excel

Selecting the "Export to Excel" link will download an excel copy of your assessment results.

NOTE: The excel report shows either Questions or Requirements. Whichever mode has more answers will show in the report.

A	B	C	D	E	F	G	H	I	J	K	L	M	N
Question_Id	Question_Group_Heading	Simple_Question	Answer_Text	Mark_For_Review	Is_Question	Is_Requirement	Is_Component	Is_Framework	Component_Id	Answer_Id	Comment	Alternate_Justification	Compc
1		The facility should have documented and distributed: 1. Cyber security policies (including a change management policy). 2. Plans/processes and supporting procedures commensurate with the facility's current IT operating environment.											
2	6223 Policies Procedures General	The facility should designate one or more individuals to manage cyber security who can demonstrate proficiency through a combination of training, education, and/or experience sufficient to develop cyber security policies and procedures and ensure compliance with all applicable industry and governmental cyber security requirements.	Y	False	False	True	False	False	0	38360			
3	6224 Policies Procedures General	The facility should identify and document systems boundaries (i.e., the electronic perimeter) and has implemented security controls to limit access across those boundaries.	Y	False	False	True	False	False	0	38361			
4	6225 Access Control	The facility should establish and document a business requirement for every external connection to/from its critical systems. The facility external connections should have controls that permit access only to authorized and authenticated users.	N	False	False	True	False	False	0	38362			
5	6226 Access Control	The facility should practice the concept of least privilege.	NA	False	False	True	False	False	0	38363			
6	6227 Access Control	The facility should practice the concept of least privilege.	A	False	False	True	False	False	0	38364			

Figure: Export to Excel Output

Import Module

NOTE: The Import New Module is designed for Developer use. The user needs experience with either JSON or XML.

There are a few different options to import a new Questions or Requirements set in CSET. The user can use an edit an existing standard, create their own JSON or XML module in CSET, or use a schema in an outside code editor and paste in CSET.

The parts of the Import New Module can be seen in the figure below.

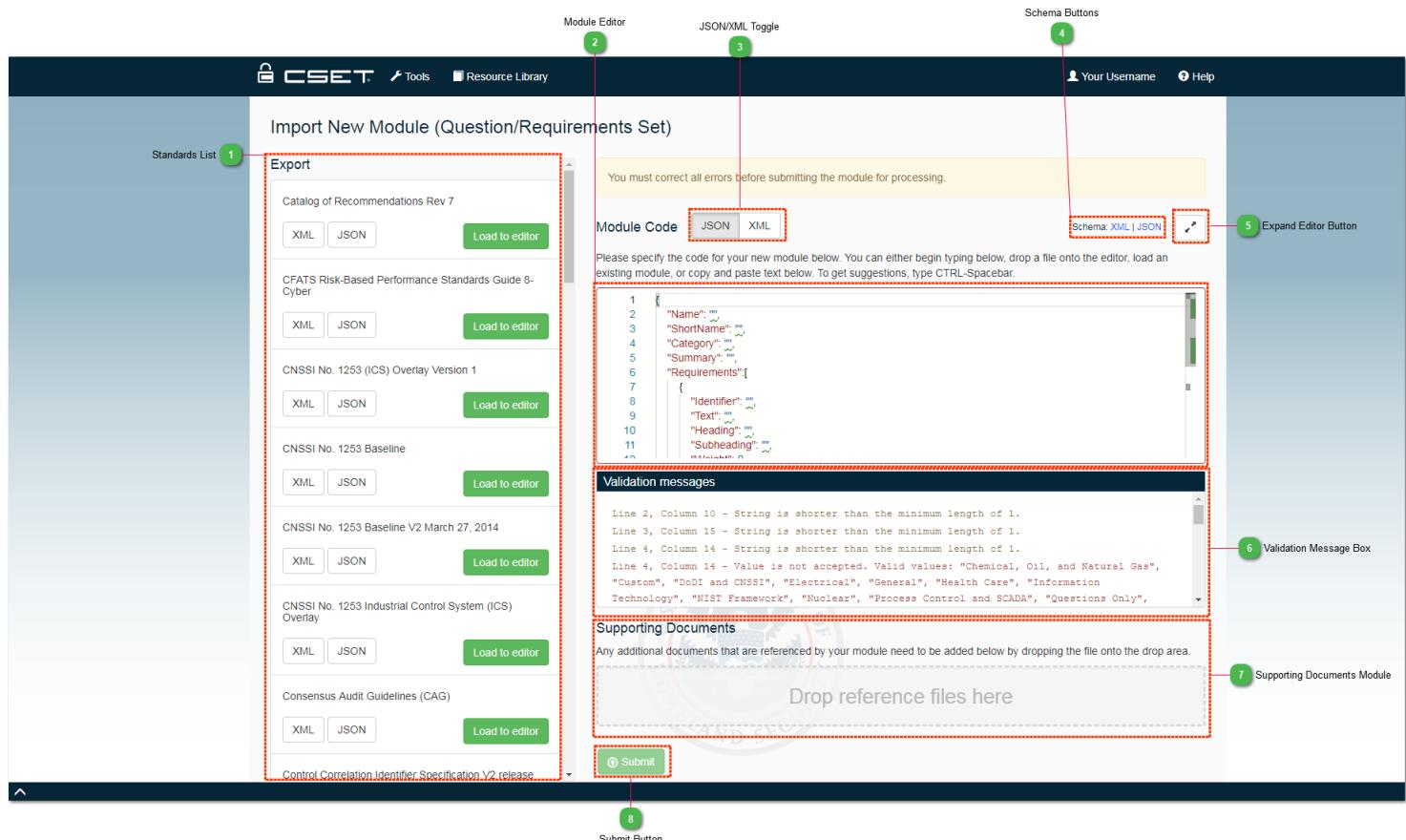


Figure: Import New Module screen

1 Standards List

Export

Catalog of Recommendations Rev 7

CFATS Risk-Based Performance Standards Guide 8-Cyber

CNSSI No. 1253 (ICS) Overlay Version 1

CNSSI No. 1253 Baseline

CNSSI No. 1253 Baseline V2 March 27, 2014

CNSSI No. 1253 Industrial Control System (ICS) Overlay

Consensus Audit Guidelines (CAG)

Control Correlation Identifier Specification V2 release

The Standards List allows the user to export any of the standard code in either XML or JSON. It also allows the user to click "Load to editor" to load any standard code to the Module Editor where it can be edited. When a new standard is imported it will show in the Standard List, as well as, the Cybersecurity Standards page.

Module Editor

2

```

1 [
2   {
3     "Name": "...",
4     "ShortName": "...",
5     "Category": "...",
6     "Summary": "...",
7     "Requirements": [
8       {
9         "Identifier": "...",
10        "Text": "...",
11        "Heading": "...",
12        "Subheading": "...",
13      }
14    ]
15  }
16]
```

The Module Editor is where the user can edit or create a new standard for import. Edit within the tool or drag and drop a file to the editor.

Tip: Use CTRL+Spacebar to see list options while coding. Use ALT+Shift+F to format code when loaded from the Standards List.

Note: New Standards can contain both Questions and Requirements. If only using Requirements they will be duplicated for the Questions set.

Short Names must be unique when editing a previously used standard.

3

JSON/XML Toggle

[JSON](#) [XML](#)

Use the JSON/XML Toggle to pick what language to use for the new standard being imported. It is recommended to use JSON, because CSET has more comprehensive validation and list options within the editor.

4

Schema Buttons

Schema: [XML](#) | [JSON](#)

Use the Schema button to download a code schema to edit in an outside editor. Drag and drop the file when complete to see validation messages and submit.

5

Expand Editor Button



Click the Expand button to expand the Module Editor to the full-screen.

6

Validation Message Box

Validation messages

```
Line 2, Column 10 - String is shorter than the minimum length of 1.
Line 3, Column 15 - String is shorter than the minimum length of 1.
Line 4, Column 14 - String is shorter than the minimum length of 1.
Line 4, Column 14 - Value is not accepted. Valid values: "Chemical, Oil, and Natural Gas",
"Custom", "DoDI and CNSSI", "Electrical", "General", "Health Care", "Information
Technology", "NIST Framework", "Nuclear", "Process Control and SCADA", "Questions Only",
```

The Validation Message box shows errors in the code, as well as, processing errors.

7

Supporting Documents Module

Supporting Documents

Any additional documents that are referenced by your module need to be added below by dropping the file onto the drop area.

Drop reference files here

Users can add supporting documents and references with the newly created standard. Drop reference files into the reference file drop area, enter a title, and a short name. Use the red trash icon or remove all to delete supporting documents.

Tip: If using the Destinations field in the editor to direct a user to a certain place in the supporting document, then the destinations must be set up in the support document itself. See [Choose Your Destination](#) for more information.

8

Submit Button



Select "Submit" when the module code is complete and ready to be created.

Module Builder

The Module Builder allows the user to create a custom Standard or Question Set.

Module List

The Module List displays all custom modules. A custom module is one that is not included in the CSET application.

The screenshot shows the CSET interface with a dark header bar containing the CSET logo and a 'Help' button. Below the header is a navigation bar with a 'Home' link. The main content area is titled 'Standard And Question Set Builder' and contains the following elements:

- A blue button labeled '+ Create Module'.
- A list of three modules:
 - 800-53 Revision 7
 - Question Set 17-A
 - Branch Office Working Standard 1.7
- A row of six icons for cloning and deleting modules:
 - Clone (Icon: square)
 - Delete (Icon: trash can)
 - Clone (Icon: square)
 - Delete (Icon: trash can)
 - Clone (Icon: square)
 - Delete (Icon: trash can)

Figure: Module list



Clone Button [Clone](#)
A module can be cloned by clicking this button. A deep copy of the module is created including requirements and questions. The source module's title is copied to the new clone, appending "(copy)". The user is transferred to the Module Detail page for the new clone.



Delete Button [Delete](#)
A custom module may be deleted, provided that no other modules have requirements based on it. This is enforced to maintain data integrity.



Create Module Button
Clicking the Create Module button will start the construction of a new module. The user is transferred to the Module Detail page.

Create a New Module

After clicking the "Create Module" button the Module Detail screen will open.

Module Detail

The Module Detail screen contains basic information about the module, such as name and description.

The screenshot shows the 'Module Detail' screen of the CSET application. At the top, there is a navigation bar with the CSET logo and a 'Help' link. Below the navigation bar, the breadcrumb trail shows 'Home > Module Detail'. The main content area is titled 'Module Detail'. It contains the following fields:

- Module Name ***: A text input field containing '800-53 Revision 7'.
- Short Name ***: A text input field containing '800-53 R7'.
- Description ***: A text area containing the following text:

This standard provides a catalog of security and privacy controls for federal information systems and organizations and a process for selecting controls to protect organizational operations, organizational assets, individuals, other organizations, and the Nation from a diverse set of threats including hostile cyber attacks, natural disasters, structural failures, and human errors.
- Category**: A dropdown menu currently set to 'Information Technology'.

At the bottom of the screen are three buttons:

- Requirements** (highlighted in blue)
- Questions**
- Manage Documents**

Figure: Module Detail screen

Requirements Button

Clicking the Requirements button will show the Requirement Listing screen.

Questions Button

Clicking the Questions button will show the Questions List screen.

Manage Documents

Clicking the Manage Documents button will show the Standard Documents screen.

Add Requirements

Clicking the Requirements button opens the Requirement Listing screen where the user can add a new requirement to their set.

The screenshot shows the CSET interface with the title "Requirement Listing". Below it, a section titled "800-53 Revision 7" contains a descriptive text about security and privacy controls. A prominent button labeled "+ Create Requirement" is visible. The main content area is titled "Access Control" and includes a sub-section "Access Control Policy And Procedures". Under this, a specific requirement "AC-1" is listed with detailed steps. To the right of the requirement text are "Edit" and "Delete" icons.

This standard provides a catalog of security and privacy controls for federal information systems and organizations and a process for selecting controls to protect organizational operations, organizational assets, individuals, other organizations, and the Nation from a diverse set of threats including hostile cyber attacks, natural disasters, structural failures, and human errors.

+ Create Requirement

Access Control

Access Control Policy And Procedures

AC-1

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. An access control policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the access control policy and the associated access controls; b. Designate an [Assignment: organization-defined senior management official] to manage the access control policy and procedures; c. Review and update the current access control: 1. Policy [Assignment: organization-defined frequency]; and 2. Procedures [Assignment: organization-defined frequency]; d. Ensure that the access control procedures implement the access control policy and controls; and e. Develop, document, and implement remediation actions for violations of the access control policy.

Edit Delete

Figure: Requirement Listing screen

Select the Create Requirement button to open the Add requirement dialogue.



Add Requirement

Category and Subcategory are used to group Requirements in CSET. Question Group Heading and Subcategory are used to group related questions.

Category

Question Group Heading

Subcategory

Title/Identifier

Requirement Text

Create

Cancel

Figure: Add a Requirement dialogue

Category Drop Down List

Select or enter the control group category. Typing in this field will filter the dropdown values to matching values. For more information about question categories, see the [Assessment Categories](#) help section.

Question Group Heading Drop Down List

This is a value under which questions are grouped when displayed in CSET questions mode. For more information about question group headings, see the [Assessment Categories](#) help section.

Subcategory Drop Down List

Select or enter the control subcategory.

For more information about question subcategories, see the [Assessment Categories](#) help section.

Title/Identifier Text Box

Enter the title or identifier of the Requirement. For example, Requirement 1 (Req.1).

Requirement Text

Enter the full text of the Requirement. Line breaks are preserved for readability and are presented when answering in CSET Requirements mode.

Create button

Click the Create button to save the new requirement and jump to the Requirement Detail screen.

Requirement Detail

Requirement Detail

Category Subcategory
Account Management Audit Failure Response

Identifier/Title *

A123

Standard-Specific Requirement *

This is it.

Security Assurance Level

Select all applicable levels.

Low Moderate High Very High

Figure: Requirement Details and SAL level

The values for Identifier/Title and the Requirement text are editable on this screen as well.

Security Assurance Level

Select all Security Assurance Levels that are applicable to the Requirement.

For more information about Security Assurance Levels, see the [Security Assurance Level \(SAL\)](#) help section.

Next, add any supplemental information for the requirement.

Supplemental Information

HTML markup can be edited directly by clicking the  button.



Figure: Supplemental text box

Supplemental Information Text Box

Enter any supplemental information for the Requirement in this box. The text can be formatted using the controls and can be edited directly as HTML by clicking the  button.

References

References

Documents that define the standard or provide additional information for the requirement are attached here. If the document is a PDF with bookmarks, specifying a relevant bookmark will allow CSET to open the PDF to the target location.

To add documents to the dropdown lists, click 'Manage Documents.'

Manage Documents	
Source Documents	Bookmark
<input type="button" value="▼"/>	<input type="text"/> +
Help Documents	Bookmark
<input type="button" value="▼"/>	<input type="text"/> +

Figure: Add and manage documents

Manage Documents Button

Before a reference document can be connected to a Requirement it must first be associated with the Module. Click this button to jump to the Standard Documents List, where that connection can be made.

Source Documents Drop Down List

A Source Document is the primary location that supplies the Requirement for the Standard. Documents that have been associated with this Module will be listed here.

Bookmark

Optional. CSET will render hyperlinks in the References section of the Requirements screen. For convenience, those links will open the Reference or Help document and jump directly to a pre-defined bookmark. If there is a bookmark in the document, it can be entered here. Enter the bookmark without a leading hash/pound symbol (#).

Click the '+' button to add the reference to the Requirement. Multiple references can be added to a Requirement.

Help Documents

A Help Document is a secondary source of information that may be helpful to the assessor to help understand a Requirement. They are added the same way as Source Documents, and are listed separately on the Requirements screen in CSET.

At this point the user can add simple questions to the individual requirement, so that they can utilize both Questions and Requirements mode. (This is not required)

To learn more about Questions/Requirements mode, see the [Mode Selection](#) help section.

Related Questions

Questions may be added to the requirement. When the standard is reviewed in CSET the assessors may choose to answer questions instead of the requirement.

+ Add Question

No questions are defined for this requirement.

Figure: Add related questions

For more information about Questions, see the [Mode Selection](#) help section.

Add Questions

A user can begin adding questions to a requirement through the Requirement Details screen. The Related Questions section is found at the bottom of the page.

To learn more about the Requirements Details screen, see the [Add Requirements](#) help section.

Related Questions

Questions may be added to the requirement. When the standard is reviewed in CSET the assessors may choose to answer questions instead of the requirement.

[+ Add Question](#)

No questions are defined for this requirement.

Figure: Add related questions

Questions can be assigned to a Requirement in order to define a question-based answer capture. This screen allows new questions to be written and attached, or questions can be pulled from the extensive set of questions defined in CSET.

For more information about Questions, see the [Mode Selection](#) help section.

Write New Question

If a question is needed that is not already defined in CSET, it may be created as shown in the figure below.

Write New Question

If you wish to add a custom question to the set, enter it here.

Categorization

Question Group Heading Subcategory

--Select Heading--

Security Assurance Level

Select all applicable levels.

Low Moderate High Very High

[Add New Question](#)

Figure: Write new question dialogue

Question Text Box

Write the text of the new question here.

Question Group Heading Drop Down List

Select a Question Group Heading that categorizes the question.

Subcategory

Select or enter the control subcategory.

Security Assurance Level

Select all Security Assurance Levels that are applicable to the Question.

Add New Question

Add New Question Button

Click to create the new question.

Search for Existing Questions

Enter keywords that would appear in the relevant question(s) and click the Search button. A list of candidates will be rendered. More words in the query will yield a smaller resulting set of questions.

Each question will display its Question Group Heading and Subcategory values, along with the Security Assurance Levels defined for the question in its original Module. You can leave them set as-is or change them as appropriate for the new Requirement.

The screenshot shows a search interface for finding existing questions. At the top, there is a search bar containing the text "authorization boundary" and a blue "Search" button with a magnifying glass icon. Below the search bar is a grey button labeled "Add Selected Questions". A light blue banner below the search bar states "8 questions were found". The main content area displays two questions. Each question has a title, group heading, subcategory, security assurance level, and a selection of applicable levels. The first question is: "Does the security plan explicitly define the authorization boundary of the system?". It has a "Group Heading: Plans" and "Subcategory: Security Plan". It includes a "Security Assurance Level" section with options "Low", "Moderate", "High", and "Very High", where "Low" is highlighted in blue. The second question is: "Does the organization develop and document an inventory of information system components that includes all components within the authorization boundary of the information system?". It has a "Group Heading: Configuration Management" and "Subcategory: Information System Component Inventory". It also includes a "Security Assurance Level" section with the same four options, where "Low" is highlighted in blue. Each question has a small grey "+" button to its right.

authorization boundary

Search

Add Selected Questions

8 questions were found

Does the security plan explicitly define the authorization boundary of the system?

+

Group Heading: Plans
Subcategory: Security Plan

Security Assurance Level

Select all applicable levels.

Low Moderate High Very High

Does the organization develop and document an inventory of information system components that includes all components within the authorization boundary of the information system?

+

Group Heading: Configuration Management
Subcategory: Information System Component Inventory

Security Assurance Level

Select all applicable levels.

Low Moderate High Very High

Figure: Searching for existing questions

Click the '+' button for each question that you wish to attach to the Requirement. Then click 'Add Selected Questions.'

Manage Documents

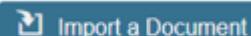
Standard Documents List

The Standard Documents screen lists all reference documents that are delivered with CSET or have been added to support custom modules.

The screenshot shows the 'Standard Documents' section of the CSET interface. At the top, there's a navigation bar with 'CSET' and a 'Help' link. Below it, a breadcrumb trail shows 'Home > Module Detail > Manage Documents'. The main title 'Standard Documents' is followed by '800-53 Revision 7'. A descriptive text block says: 'Select or upload any reference documents applicable to the standard. This will make them available for attaching to the requirements in the standard. Enter a string in the Filter field to narrow down candidates.' To the right is a blue button labeled 'Import a Document' with a file icon. Below this, there's a 'Filter' input field and a checkbox for 'Show Selected Items'. The main area is a table with two columns: 'Title' and 'File Name'. The table contains the following data:

Title	File Name
14 CFR 121.368 Certificate Holder	14cfr121-368.pdf
14 CFR Parts 43.11	14 CFR Parts 43.11.pdf
14CFR Part 121.380	14CFR Part 121.380.pdf
14CFR Part 135.439	14CFR Part 135.439.pdf
14CFR Part 43.3	14CFR Part 43.3.pdf
21 Steps to Improve Cyber Security of SCADA Networks_DOE	21_Steps-SCADA.pdf
73.2 Definitions	NRC_10CFR73.2Definitions.pdf

Figure: Standards document list



Import a Document Button

Opens a dialog to select a reference document for upload.

Filter

Typing in this field will trim the displayed list of documents to make it easier to locate the desired document.

List checkboxes

Any documents that should be available to associate with a Requirement, either as a Source Document or Help Document can be checked in this list.

NOTE: Checking a document in this list only makes the document available for inclusion when defining Requirements. To add a document to a Requirement, see the instructions for the [Requirement Detail](#) page.

Resource Library

The Resource Library is an excellent way to help the user better understand and resolve the concerns identified by the assessment and to improve the security of the user's systems. It contains a variety of standards, reports, templates, white papers, plans, and other cybersecurity-related documents. The figure below shows the Resource Library window.

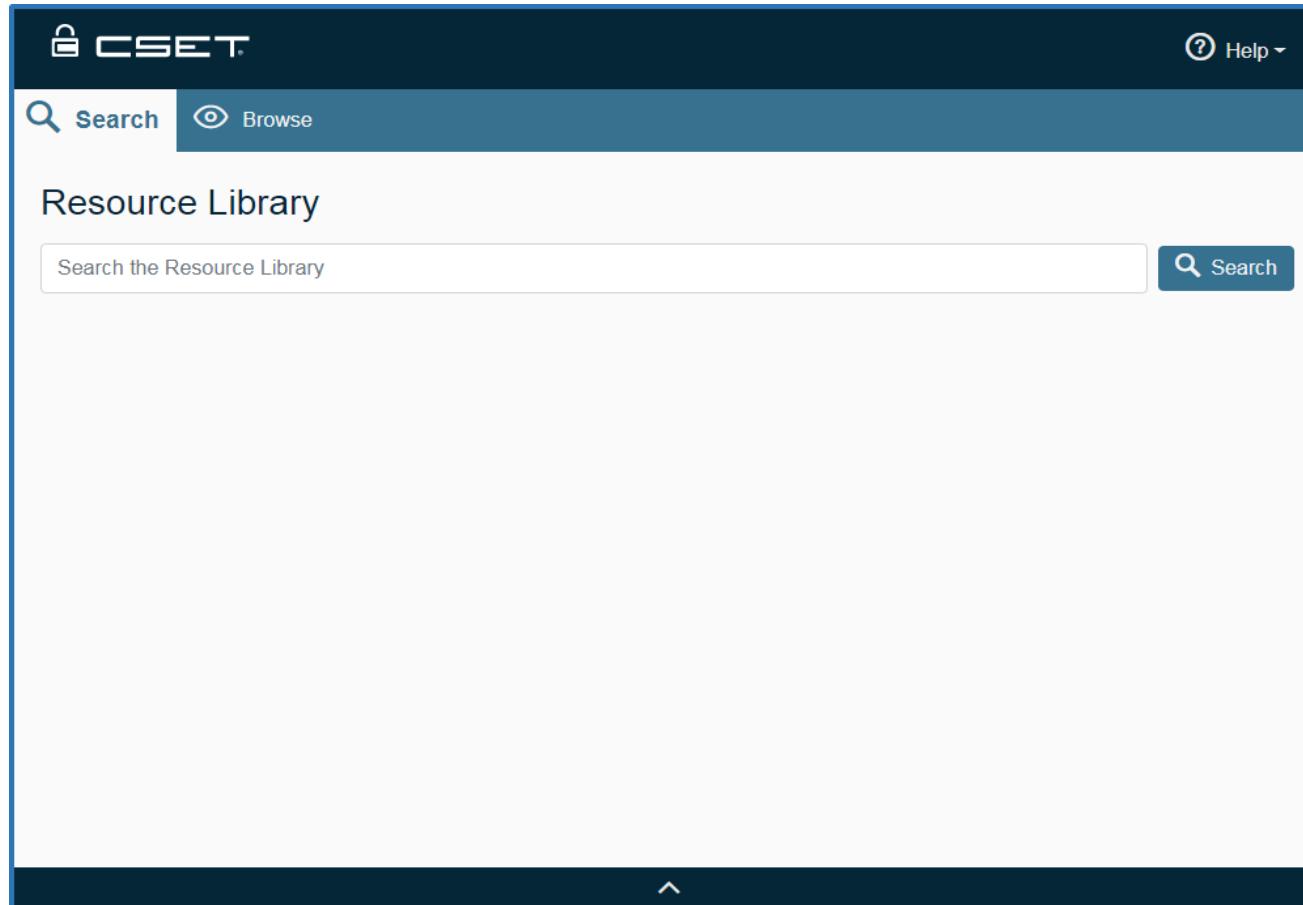


Figure: Resource Library window

Search Screen

Two ways are available to find documents within the Resource Library. This section discusses the Search feature. The other way is by using the document tree structure discussed in the help section titled [Browse Screen](#).

The Search screen option of the Resource Library provides a way to find a list of documents based on the text string typed into the search box. Clicking the Search tab opens a search box. Enter the desired text string and click on the magnifying glass icon or press the keyboard Enter key to begin the search.

The figure below shows an example where the user has typed in the string "contingency." In this case, CSET searches through all the documents for occurrences of the word "contingency" and then ranks and presents them in an ordered list in the Search Results.

The screenshot shows the CSET Resource Library search interface. At the top, there is a navigation bar with the CSET logo, a Help button, and tabs for 'Search' and 'Browse'. The 'Search' tab is active. Below the navigation bar, the title 'Resource Library' is displayed. A search bar contains the query 'contingency'. To the right of the search bar is a blue 'Search' button with a magnifying glass icon. The main area is titled 'Results:' and lists two items:

- Contingency Plan Template - NIST**
Contingency Plan Template - NIST
This document provides a NIST template for preparing a contingency plan. Downloaded from:
http://csrc.nist.gov/groups/SMA/fasp/documents/contingency_planning/contingencyplan-template.doc.
ContingencyPlan_template_NIST.pdf
- Contingency Plan Template for Systems - HHS**
Contingency Plan System Template - HHS
This document provides a Dept. of Health and Human Services (HHS) template for preparing a system level contingency plan.
Downloaded from: <http://www.hhs.gov/ocio/securityprivacy/incidentmanagement/incidentresp.html>.
ContingencyPlan_system_template_HHS.pdf

Figure: Resource Library Search screen

Search tab: Clicking the Search tab will display the search functions of the Resource Library. The Resource Library always opens to the Search tab.

Search bar: The Search bar allows the user to enter keywords related to the desired documents. The user enters one or more keywords and clicks the Search button or presses the "Enter" key on the keyboard to perform the search. Results of the search are displayed in the Search Results list.

Search Results List: The Search Results list displays the documents found by the Search. Once there are documents displayed, the user can click a document to see the contents in a new tab.

Wildcards

There are two different types of wildcard characters that can be used in the search. The first is the asterisk character that can be used to substitute for one or more characters. For example, if entering the text "fire*", the search would look for anything starting with those characters and the user would see a prioritized list starting with topics related to firewalls. Without the asterisk the search would look for "fire" and the first entry would be Fire Protection.

Exact characters could also be substituted with question marks. For example, entering the text "NIST SP800-???" will return the NIST Special Publication 800 series documents where the last two characters are substituted by the wildcard character.

When CSET is searching for the text string, it is evaluating both the title and the content of the document. While the search will evaluate any character string, it is recommended that the entry be as specific as possible to limit and refine the list. The search is not sophisticated enough to find similar or close spellings. A misspelled word like "*Ciber-Security*" will return no results.

Topic Searches

In most cases, the user will be searching for a specific subject; however, the search capability can also be used to search for types of documents. In the example above, the returned document is a DHS recommended practice. By entering "recommended practice" in the search text box, the user can create a list of all the recommended practices developed by DHS as well as other documents that may use that phrase.

Browse Screen

Two ways are available to find documents within the Resource Library. The first is by using the Search screen discussed in the help section titled [Search Screen](#). The second is by using the document tree structure shown in the figure below.

In the document tree structure, all the topics in the library are organized in a hierarchical format and displayed as leaf nodes on one or more branches, with a branch representing a topic. Each main topic can be expanded to more detailed subtopics until only the list of documents remains. The branches may be one or several levels deep.

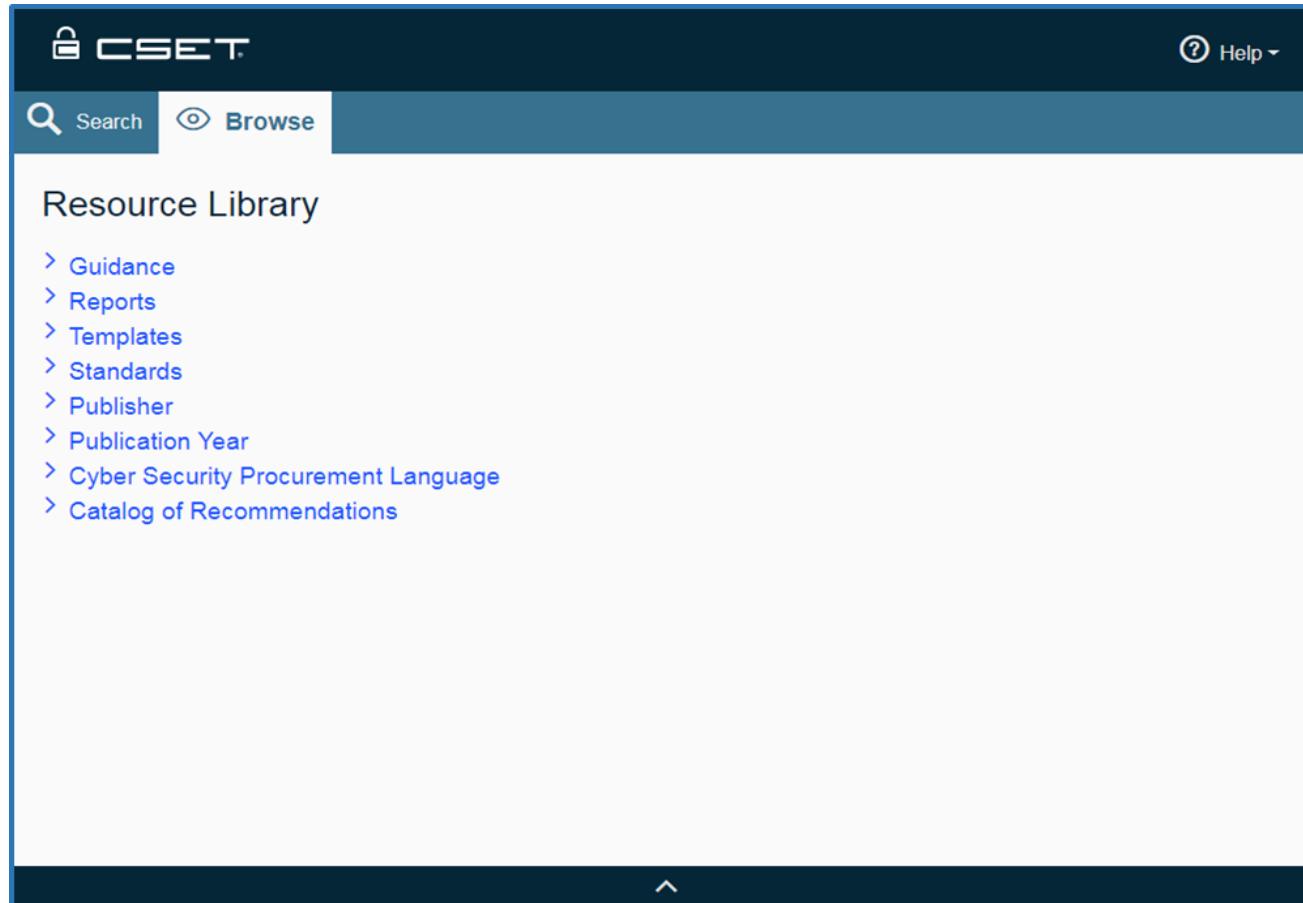


Figure: Resource Library document tree

Document Tree List: The Document Tree list displays the documents in the Resource Library organized by category in an expandable tree structure. The tree structure contains branches (Categories) and Leaves (Documents). Branches can be clicked to show more branches or leaves. Leaves can be clicked to display selected documents in a new tab.

[Search](#)[Browse](#)

Resource Library

- > Guidance
- > Reports
- > Templates
- ▽ Standards
 - ▽ Access Control

[FIPS 201-1 PIV Employees Contractors](#)

This standard specifies the architecture and technical requirements for a common identification standard for Federal employees and contractors. The overall goal is to achieve appropriate security assurance for multiple applications by efficiently verifying the claimed identity of individuals seeking physical access to Federally controlled government facilities and electronic access to government information systems.

[ICD 704 Personnel Controlled Access](#)

The directive establishes Director of National Intelligence (DNI) personnel security policy governing eligibility for access to Sensitive Compartmented Information (SCI) and information protected within other controlled access programs.

[NIST SP800-73 Personal Identity Verification](#)

SP 800-73-3 contains the technical specifications to interface with smart cards to retrieve and use identity credentials. The specifications are described in 4 parts and reflect the design goals of interoperability and PIV Card functions. The goals are addressed by specifying the PIV data model, card edge interface, and application programming interface.

Figure: Expanded document tree

In the example shown in the figure above, the Access Control branch under Standards was clicked to open and expose the documents that are found under it. Any document selected will open in a new tab for the user to read.

The options to browse by publisher and publication year are also available. They were added for those users looking for specific versions of documents or documents from a specific source. The documents listed under these headings are the same as in the rest of the tree but listed in a differing order.

The final two subjects in the tree labeled Cyber Security Procurement Language and Catalog of Recommendations are unique and will open special access to the content rather than the files themselves.

[Cyber Security Procurement Language:](#)

By clicking the branch labeled Cyber Security Procurement Language, the screen expands the tree to show the topics in the Procurement Language document. (The full document can be found using the Search or Document Tree methods.) The figure below shows the branch open with the topic Removal of Unnecessary Services and Programs displayed (found under the System Hardening category).

Removal of Unnecessary Services and Programs

System hardening is a security principle that should be considered when designing and procuring control systems products. It refers to making changes to the default configuration of a Network Device and its operating system (OS), software applications, and required third-party software to limit security vulnerabilities. Removal of unnecessary services and programs is an aspect of system hardening that refers to removal of unnecessary services and programs commonly installed on network devices.

Basis

Unused services in a host operating system that are left enabled are possible entry points for exploits on the network and are generally not monitored because these services are not used. Only the services used for control systems operation and maintenance shall be enabled to limit possible entry points.

Language Guidance

Often, networked devices ship with a variety of services enabled and default operating system programs/utilities pre-installed. These range from system diagnostics to chat programs, several of which have well-known vulnerabilities. Various attacks have been crafted to exploit these services to obtain information leading to compromise the system.

Any program that offers a network service that "listens" on specific addresses for connection requests. On a Transmission Control Protocol (TCP)/Internet Protocol (IP) network, these addresses are a combination of IP address and TCP or User Datagram Protocol (UDP) ports. A recommended hardening activity is simply disabling or removing any services or programs, which are not required for normal system operation, thus removing potential vulnerabilities.

Port scans are the normal method of ensuring existence of required services and absence of unneeded services. A port scan shall be run before the FAT with a representative, fully functional system configuration. All input/output (I/O) ports need to be scanned for UDP and TCP. The scan needs to be run before the FAT and again prior to the SAT. Port scans can rarely be used on production systems. In most cases, scanners will disrupt operations.

Procurement Language

Postcontract award, the Vendor shall provide documentation detailing all applications, utilities, system services, scripts, configuration files, databases, and all other software required and the appropriate configurations, including revisions and/or patch levels for each of the computer systems associated with the control system.

The Vendor shall provide a listing of services required for any computer system running control system applications or required to interface the control system applications. The listing shall include all ports and services required for normal operation as well as any other ports and services required for emergency operation. The listing shall also include an explanation or cross reference to justify why each service is necessary for operation.

OK

Figure: Cyber Security procurement language

In this case, instead of a document being opened, CSET displays formatted text taken directly from the Cyber Security Procurement Language document.

Each topic includes some or all the following sections:

- Brief Overview of the Topic,
- Basis,
- Language Guidance,
- Procurement Language,
- Factory Acceptance Test (FAT) Measures,
- Site Acceptance Test (SAT) Measures,
- Maintenance Guidance,
- Dependencies, and
- References.

To fully understand how the procurement language was developed, how it is to be used, any limitations and constraints, and general information about the document, open the document and read the front pages. To access it, click on Search and then type in procurement language.

Catalog of Recommendations:

This first level branch will open the list of topics that are associated with the Catalog of Control Systems Security: Recommendations for Standards Developers. The figure below shows an example.

Security Policy and Procedures

Security policies are an extension of higher-level organizational policies with consideration for identified risks. Procedures implement the policies and allow the organization to communicate to employees, third party contractors, and vendors how the security program will be managed.

Requirement

The organization develops, implements, and periodically reviews and updates:

1. *A formal, documented, control system security policy that addresses:*
 1. *The purpose of the security program as it relates to protecting the organization's personnel and assets*
 2. *The scope of the security program as it applies to all organizational staff and third-party contractors*
 3. *The roles, responsibilities, management commitment, and coordination among organizational entities of the security program to ensure compliance with the organization's security policy and other regulatory commitments.*
2. *Formal, documented procedures to implement the security policy and associated requirements. A control system security policy considers controls from each family contained in this document.*

Supplemental Guidance

The security policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The control system security policy can be included as part of the general security policy for the organization. Procedures can be developed for the security program in general and for the control system in particular, when required.

Requirement Enhancements

None

References

NIST Special Publication 800-53 Revision 3 AC-1, SC-14, PM-1

20 Critical Security Controls Twenty Critical Controls for Effective Cyber Defense: Consensus Audit CC-9

OK

Figure: Catalog of Recommendations

Development of the Catalog was originally sponsored by DHS with input from NIST and five national laboratories. It consolidated the requirements from 15 control system and information technology Standards and was intended to serve as a source of requirements and controls for the developers of ICS Standards. Because of its popularity and comprehensive ICS requirements, it has become a principal Standard in all versions of CSET and in the ICS community at large in addition to Standards developers.

To access a topic, simply click on the branch title in the tree. In the example above, Security Policy was selected and the topic Security Policy and Procedures was chosen.

On the right-hand side of the screen, CSET displays the content from the Catalog.

Each topic includes some or all the following sections:

- Brief Overview of the Topic,
- Requirement Text,
- Supplemental Guidance,
- Requirement Enhancements, and
- References.

Like the procurement language document, to fully understand the background and intent of the Catalog, open and read the front pages.

User Profile

The User Profile menu allows the user to view their User Profile Information and their assessments, Change Password, and Logout of CSET.

The "My Assessments" link will navigate the user to their landing page. To learn more about the landing page, see [CSET Landing Page](#).

The "Logout" link will log the user out and return them to the CSET home page.

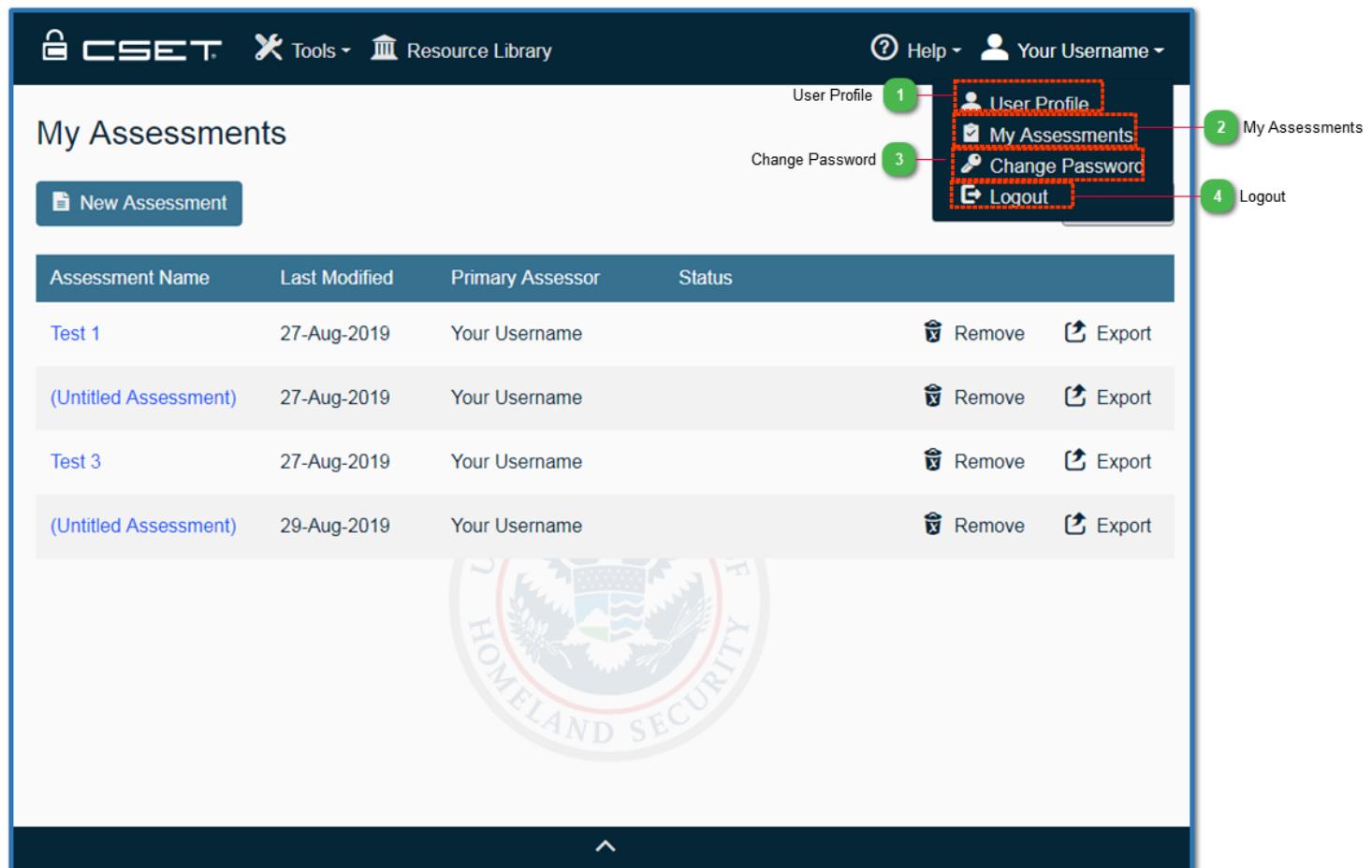
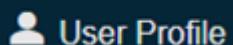


Figure: User Profile menu

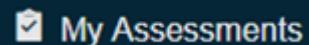
1 User Profile



Click User Profile to view and edit User Profile Information.

See [User Profile Information](#) for more information.

2 My Assessments



Click My Assessments to be directed to the user's Landing Page.

See [CSET Landing Page](#) for more information.

3 Change Password



Click Change Password to change the user's password.

See [Change Password](#) for more information.

4 Logout



Click Logout to be logged out of CSET and returned to the Home Page.

NOTE: When using the stand-alone version of CSET the only option available in the User Profile menu is "My Assessments". The User Profile menu will always be labeled "Local User".

User Profile

The User Profile menu allows the user to change their First Name, Last Name, and/or Email. The menu also provides a space for the user to choose and enter answers for security questions.

The screenshot shows a 'User Profile' dialogue box. At the top left is a user icon. The title 'User Profile' is centered above the form fields. The form consists of several input fields: 'First Name *' with placeholder 'Your', 'Last Name *' with placeholder 'Username', 'Email *' with an empty field, and 'Confirm Email *' with an empty field. Below these is a section titled 'Security Questions' with the sub-instruction: 'Providing security questions is optional but allows you to recover your password should you forget it.' It includes a dropdown labeled 'Security Question 1' and a text input labeled 'Security Answer 1'. At the bottom are two buttons: 'Save' (in a blue box) and 'Cancel'.

Security Question 1	Security Answer 1
▼	Answer

Save Cancel

Figure: Edit User Profile dialogue

The User Profile dialogue will show your profile information. Use this dialogue to change first and last name or email. Select the "Save" button to keep changes or "Cancel" to exit the dialogue.

Select a Security Question from the dropdown and type your answer in the Security Answer field. These questions will be used if you forget your password.

Change Password

Users can select the "Change Password" link to change their password.

Enter the Current Password and New Password twice to change passwords.

The screenshot shows a modal dialogue box titled "Change Password". It contains three input fields: "Current Password *", "New Password *", and "New Confirm Password *". Below the fields are two buttons: "Change Password" (in a dark blue box) and "Cancel" (in a light gray box). The entire dialogue is set against a white background.

Change Password	
Current Password *	<input type="text"/>
New Password *	<input type="text"/>
New Confirm Password *	<input type="text"/>
<input type="button" value="Change Password"/>	<input type="button" value="Cancel"/>

Figure: Change Password dialogue

Help Menu

The Help Menu shown in the figure below allows the user to access help documentation for the CSET tool.

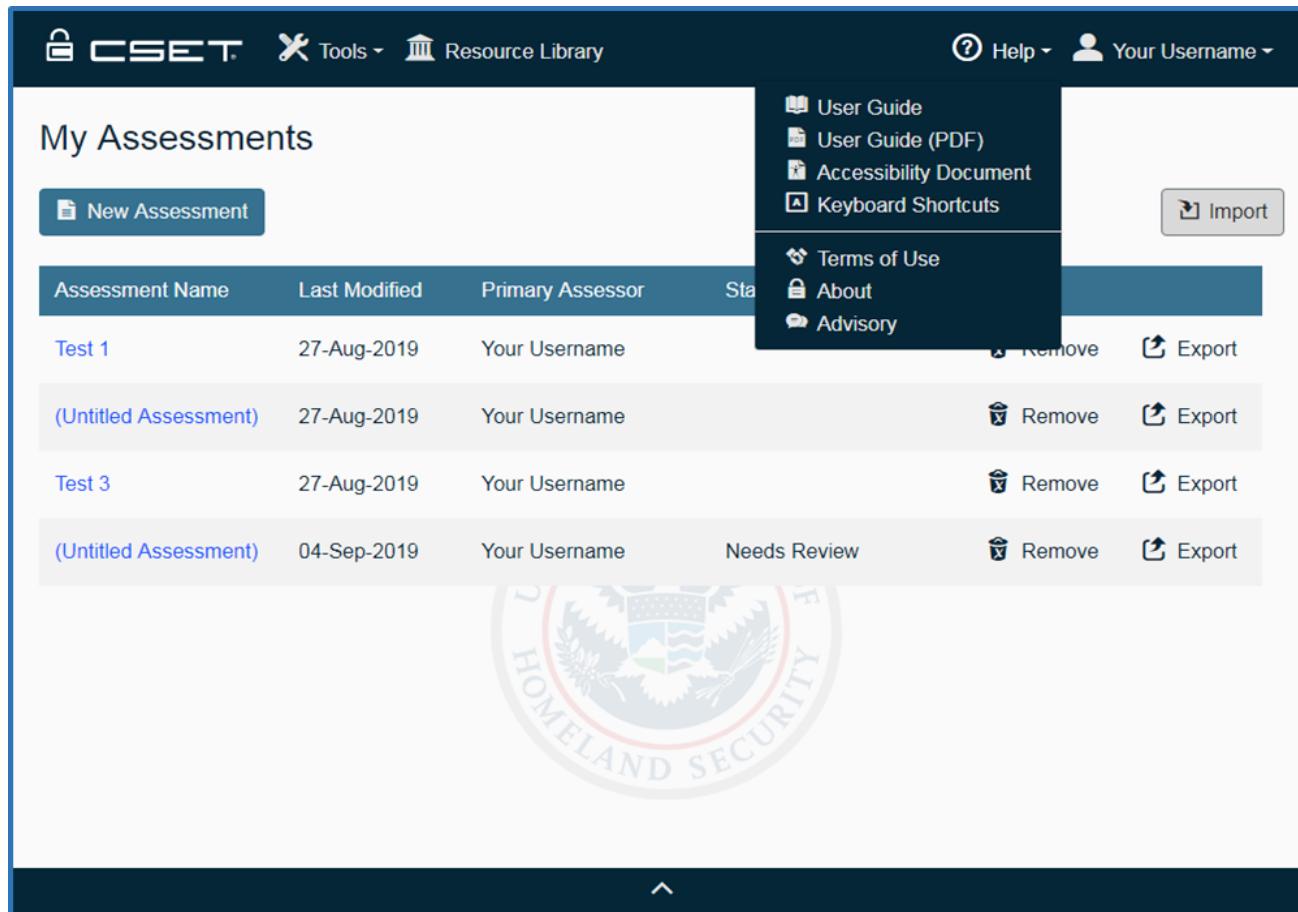


Figure: Help menu

Help Menu: Clicking the Help menu button opens the Help menu.

User Guide: Clicking the User Guide menu item will open this user guide as a CHM file containing screen shots and instructional information for using the CSET tool.

User Guide (PDF): Clicking the User Guide (PDF) menu item will open this user guide as a PDF file containing screen shots and instructional information for using the CSET tool.

Accessibility Document: Clicking the Accessibility Document menu item will open the CSET Accessibility Features Document, which describes how CSET addresses accessibility issues including the use of high contrast mode, and keyboard access.

See [Accessibility Document](#) for more information.

Keyboard Shortcuts: Clicking the Keyboard Shortcuts menu item will open the CSET Keyboard Shortcuts document, which contains a list of all keyboard shortcuts available to users of the CSET tool.

See [Keyboard Shortcuts](#) for more information.

Terms of Use: Clicking the Terms of Use menu item will open the CSET Terms of Use that describes the terms that user's agree to when using CSET.

See [Terms of Use](#) for more information.

About CSET: Clicking the About CSET menu item will open the About CSET window containing version information, web site links to videos, training and contact information for the CSET team.

See [About CSET](#) for more information.

Advisory: Clicking the Advisory menu item will open the Advisory window that contains disclaimer information.

See [Advisory](#) for more information.

CSET Accessibility Features

The figure below shows the CSET Accessibility Features document that can be accessed from the Help menu of the CSET tool.

CSET Accessibility Features

The features and functions within CSET have been developed to support application users with accessibility requirements. Industry standards have been followed to take advantage of accessibility features built into the Windows operating system and all the accessibility features supported by the browser. These combined capabilities support compliance with Section 508 of the U.S. Rehabilitation Act.

Note: The Diagram and Analysis functionality of CSET has not been made accessible or compliant to Section 508 requirements.

Diagram: Diagram utilizes an extensive list of keyboard shortcuts.

Analysis: Accessibility for the analysis functionality can be accomplished by printing the reports or producing an on-screen version of the reports. Reports are generated in .HTML format.

High Contrast Functionality

All text areas on CSET other than the Diagram and Analysis pages support switching to High Contrast mode within the Windows operating system.

Keyboard Access

CSET is accessible from the keyboard. All areas of the application other than the Analysis page can be accessed from the keyboard. Most keyboard access is implemented by using the TAB and ARROW keys for navigation, the SPACE and ENTER keys for selection. Additional shortcut or hot keys may be found in the Keyboard Shortcuts dialog.

Figure: CSET Accessibility Features document

Keyboard Shortcuts

The figure below shows the CSET Keyboard Shortcuts document that can be accessed from the Help menu of the CSET tool.

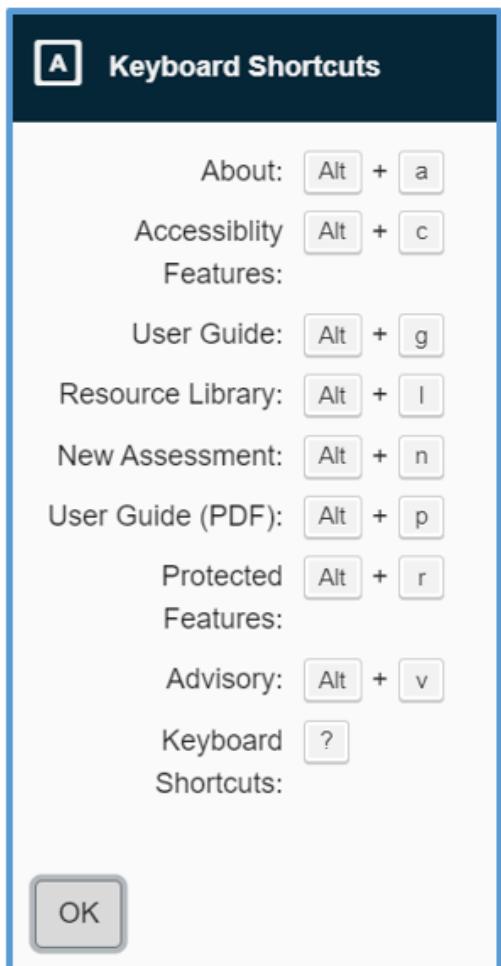


Figure: CSET Keyboard Shortcuts document

Terms of Use

The figure below shows the Terms of Use that can be accessed from the Help Menu.



Figure: Terms of Use

About CSET

The About CSET window provides the user with more information about the CSET team. The figure below points out a few important details on the About CSET window.

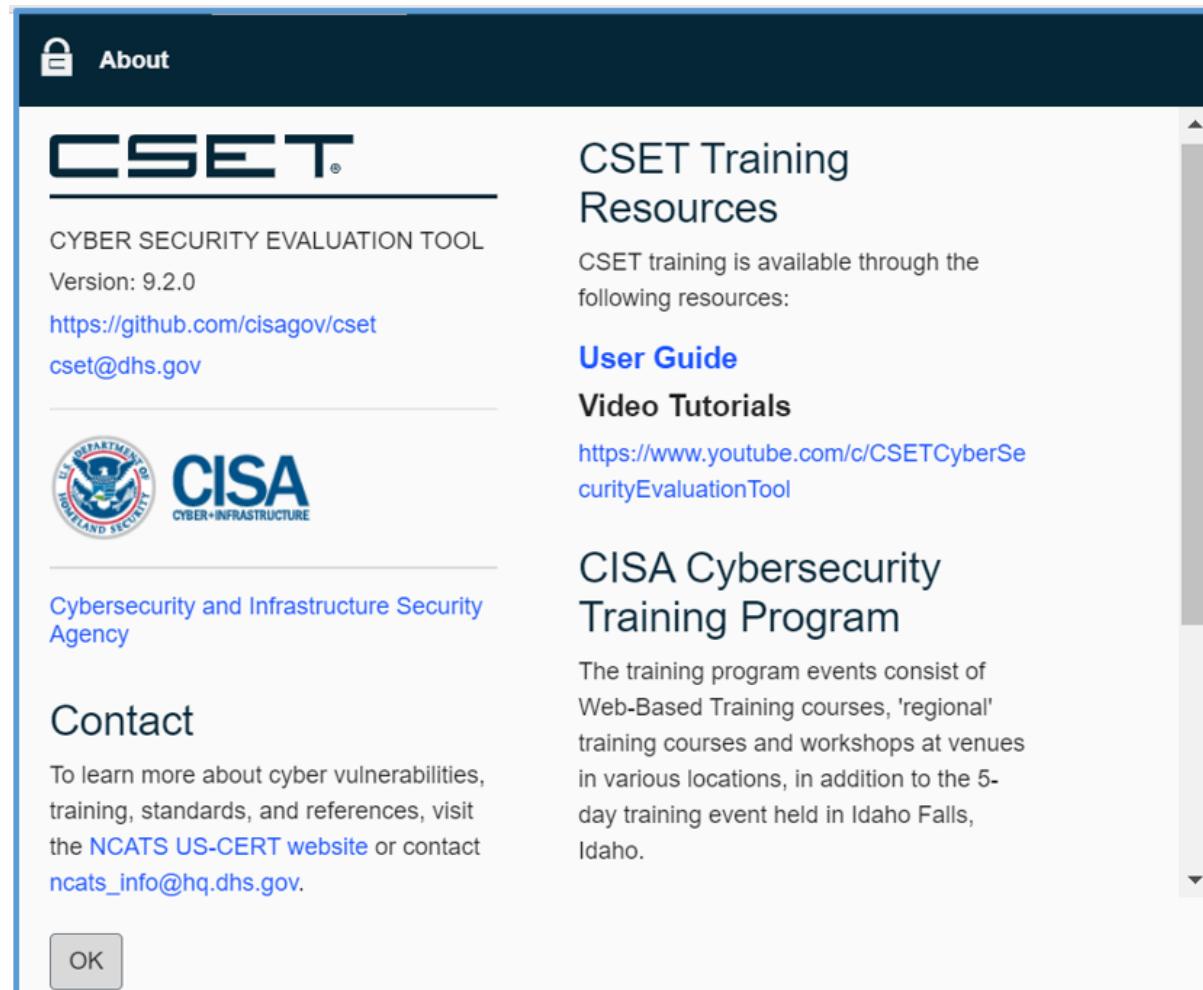


Figure: About CSET window

CSET version text: The CSET Version text indicates the current installed version of CSET. The last 4 digits indicate the build number that may be useful when communicating problems with the CSET support team.

CSET Site URL: The CSET Web Site URL is the CSET tool's web site URL where the user can learn more about the CSET tool, request features, and report defects or problems.

CSET email: The CSET email address allows the user to contact the CSET team with questions or concerns regarding the CSET tool.

Contact information: Use the links to contact a representative with questions about cyber vulnerabilities, training, standards, and references.

Video tutorials URL: The Video Tutorials URL is a URL to current CSET training videos located on YouTube.

Training information: Use the links in Training Information to find training opportunities.

OK button: Clicking the Close button will close the About CSET window

Advisory

The figure below shows the Advisory window that can be accessed from the Help menu of the CSET tool.

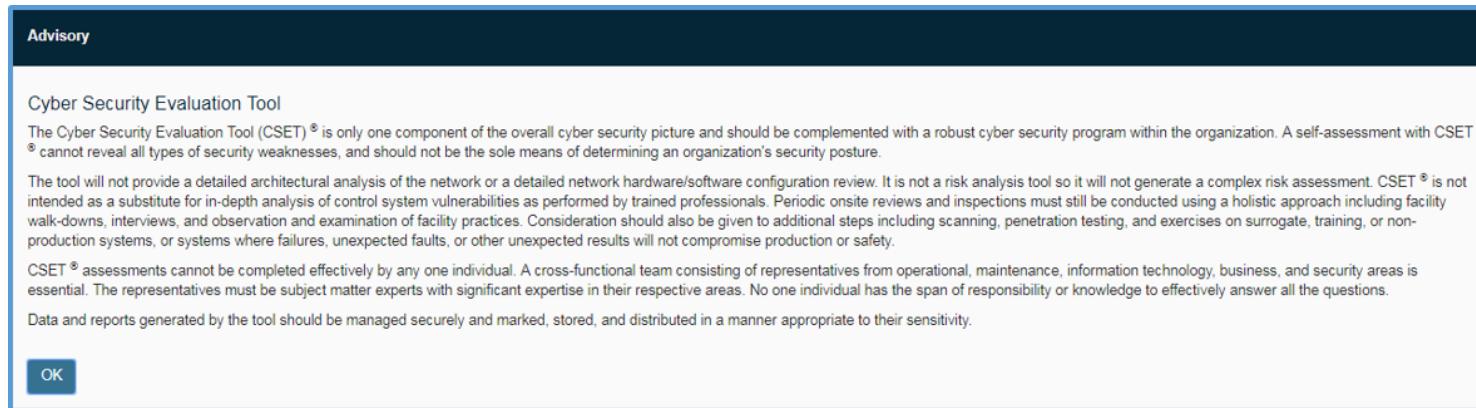


Figure: Advisory screen

Operation Menus

This section addresses the main operation menus of the CSET assessment tool. They include the Preparation menu, the Assessment menu, and the Results menu.

Preparation Menu

The Preparation menu allows quick access to the assessment preparation screens. The figure below describes the buttons and menu.

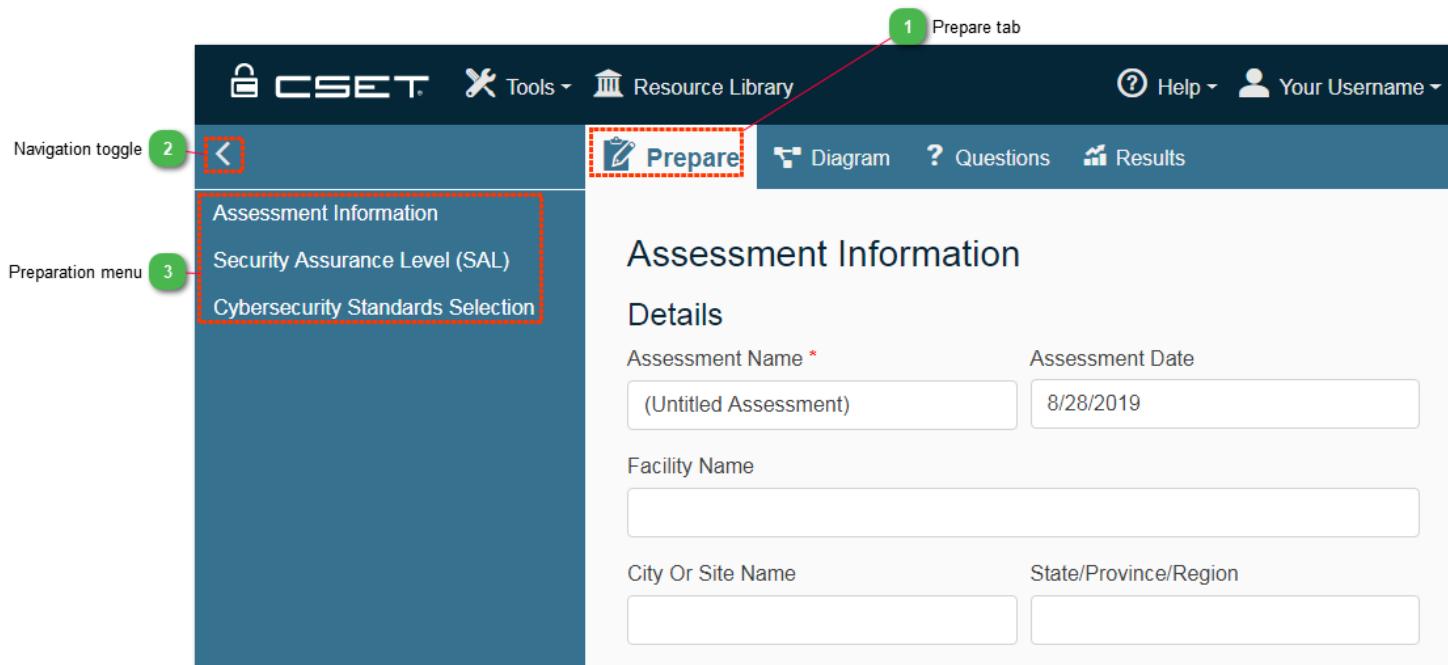


Figure: Preparation button/menu

1 Prepare tab



Clicking the Preparation button will display the Assessment Details screen.

See [Assessment Details](#) for more information.

2 Navigation toggle



Use the Navigation Toggle to open and close the Navigation Menu.

3 Preparation menu

- Assessment Information
- Security Assurance Level (SAL)
- Cybersecurity Standards Selection

The Preparation menu items indicate the screens encountered by the user during the preparation process.

See [Assessment Details](#), [Security Assurance Levels \(SAL\)](#), and [Cybersecurity Standards Selection](#) for more information.

Note: The [Cybersecurity Framework](#) menu item isn't available unless Cybersecurity Framework is the selected standard.

Diagram

The Diagram Menu is empty. To work within Diagram select "Create a network diagram" or "Edit network diagram".

The screenshot shows the CSET software interface. At the top, there is a dark header bar with the CSET logo, a 'Tools' dropdown, a 'Resource Library' link, a 'Help' link, and a 'Your Username' dropdown. Below the header is a navigation bar with links for 'Prepare', 'Diagram' (which is highlighted in blue), 'Questions', and 'Results'. The main content area has a title 'Diagram and Network Component Selection'. It contains text explaining the benefits of building a network diagram and a bulleted list of three items. At the bottom of the content area are two buttons: 'Edit the network diagram' and 'Diagram Inventory'. On the far left is a 'Back' button, and on the far right is a 'Next' button.

Figure: Diagram screen

For more information, see the [Diagram screen](#) section.

Questions Menu

The Questions menu allows quick access to the assessment questions and categories. The figure below shows the Questions menu navigation.

NOTE: Requirements mode navigation will differ in that it shows standards at the top level and then categories nested underneath them.

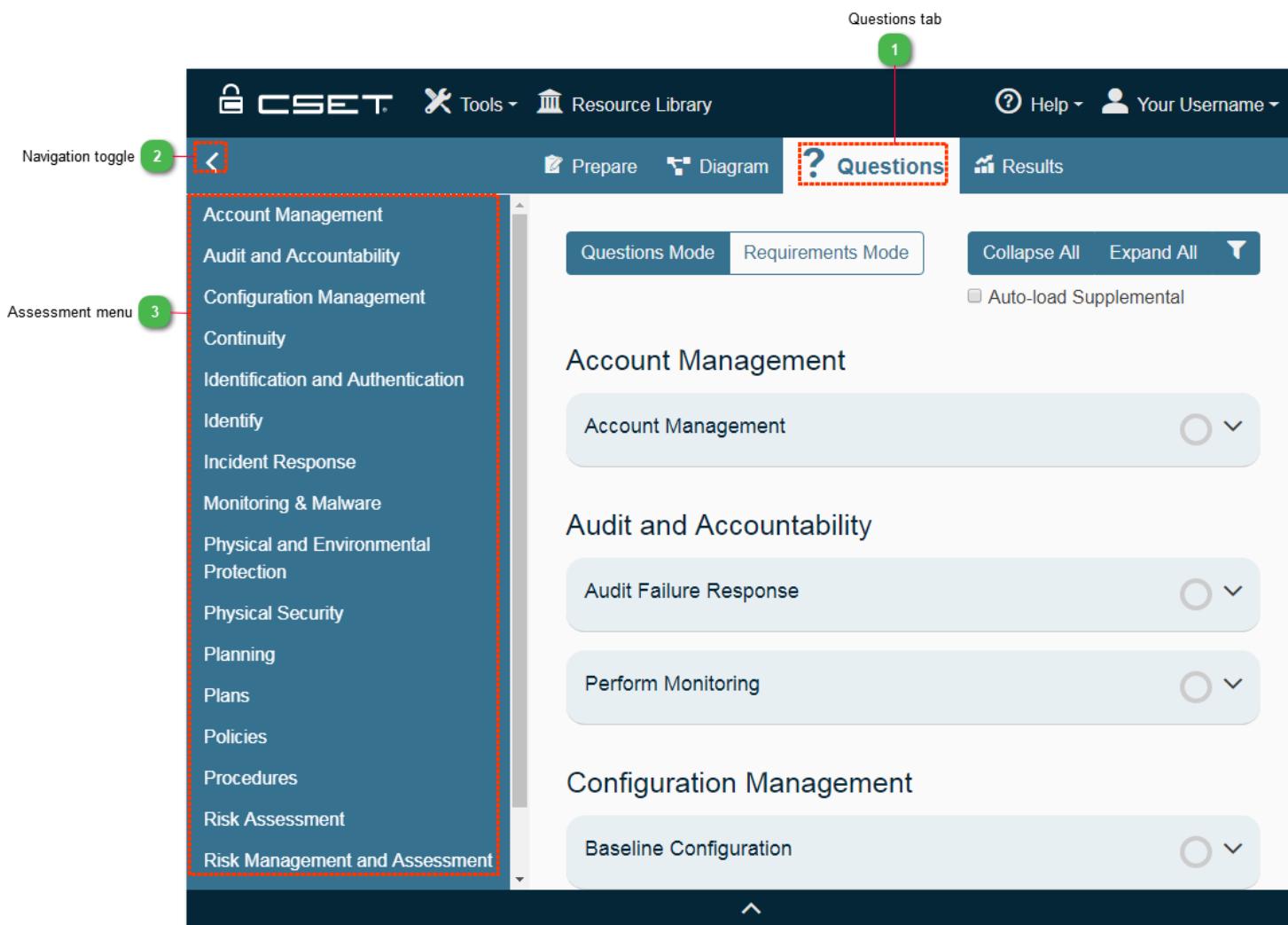


Figure: Assessment button/menu

1 Questions tab



Clicking the Questions Tab will display the Questions screen displayed after the Preparation process.

See the [Assessment Section](#) for more information about the Questions screen.

2 Navigation toggle



Use the Navigation Toggle to open and close the Navigation Menu.

Assessment menu

- Account Management
- Audit and Accountability
- Configuration Management
- Continuity
- Identification and Authentication
- Identify
- Incident Response
- Monitoring & Malware
- Physical and Environmental Protection
- Physical Security
- Planning
- Plans
- Policies
- Procedures
- Risk Assessment
- Risk Management and Assessment

The Assessment Navigation menu shows a list of all question categories awaiting completion for the assessment. The user can quickly navigate to a specific category by clicking the desired menu item.

Results Menu

The Results menu allows quick access to the assessment results and reports screens. The figure below shows the Results menu.

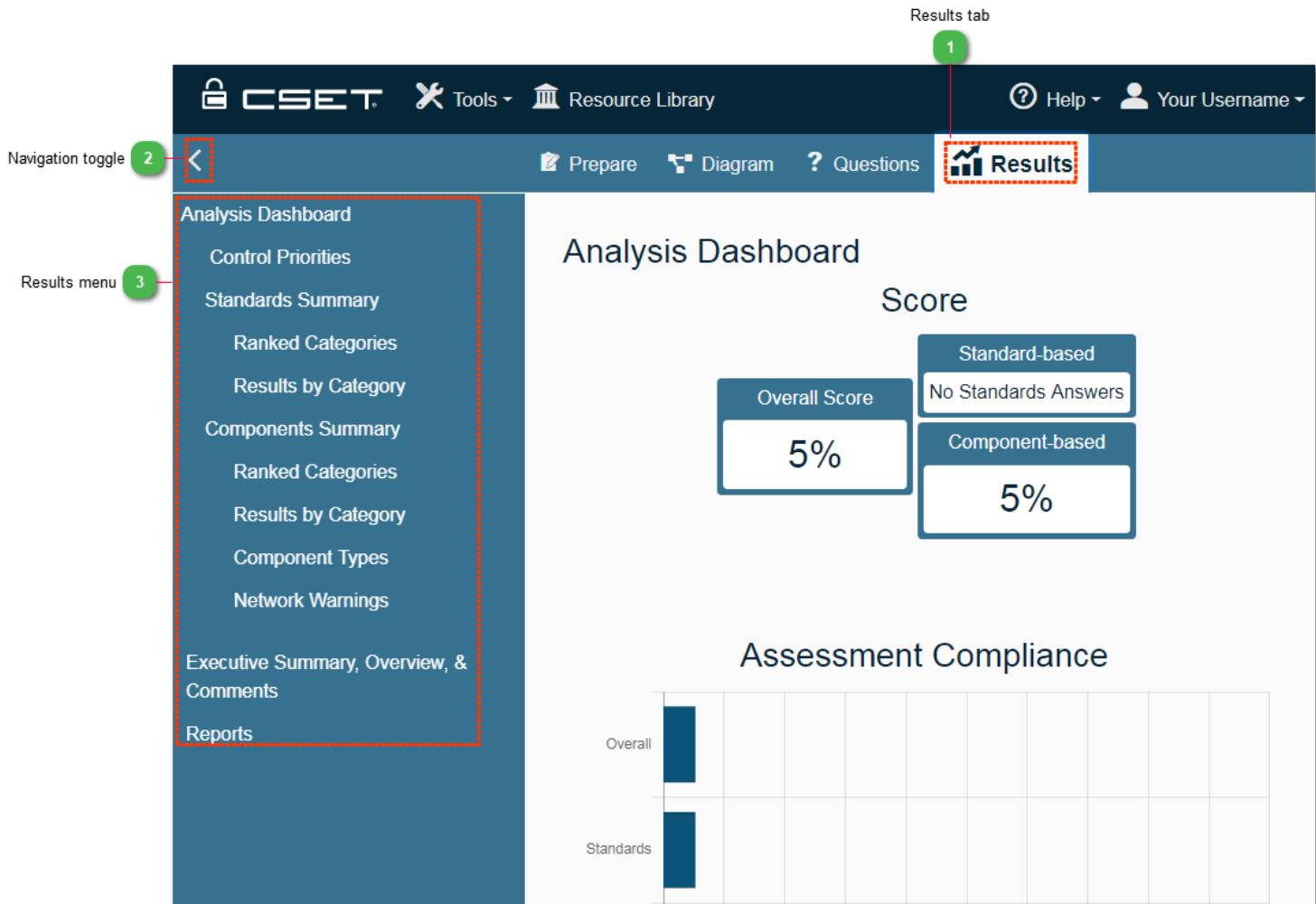


Figure: Results button/menu

1 Results tab



Clicking the Results button will display the Results Overview screen.

See the [Results Menu](#) for more information.

2 Navigation toggle



Use the Navigation toggle to open and close the Navigation Menu.

3 Results menu

Analysis Dashboard

Control Priorities

Standards Summary

Ranked Categories

Results by Category

Components Summary

Ranked Categories

Results by Category

Component Types

Network Warnings

Executive Summary, Overview, & Comments

Reports

The Results menu items indicate the screens available to the user in the main Results Section.

Main CSET Window Sections

This part of the user manual contains information about the different sections of the main CSET window including the Preparation, Diagram, Assessment, and Results sections.

Prepare Section

The Prepare section is where the assessment process begins. The preparation screens help the user to quickly get ready to answer the appropriate questions for their facility by defining the questions that will be answered during the assessment. The following pages will describe the preparation screens in more detail.

CSET Landing Page

The CSET landing page is the first screen seen after logging in. The figure below shows the CSET landing page.

The screenshot shows the CSET landing page with the following interface elements:

- Header:** CSET logo, Tools menu, Resource Library, Help, and Your Username.
- Title:** My Assessments
- New Assessment Button:** A green button labeled "1" with a red dashed box around it, pointing to the "New Assessment" button.
- Import Button:** A "Import" button in the top right corner.
- Data Table:** A table listing assessments with columns: Assessment Name, Last Modified, Primary Assessor, and Status. The table includes rows for "Test 1", "(Untitled Assessment)", "Test 3", and another "(Untitled Assessment)" entry.
- Actions:** Each row has "Remove" and "Export" buttons.
- Seal:** The U.S. Department of Homeland Security seal watermark is visible in the background.

Figure: CSET landing page

New Assessment Button



Clicking the New Assessment button will start the assessment preparation process that will allow the user to address important areas before they can begin answering questions.

The first screen of the assessment preparation process is the [Assessment Details screen](#).

Tip: All the landing page columns can be sorted by clicking the arrow next to the column name.

Assessment Details

Clicking the Assessment Details menu item in the Preparation Menu opens the Assessment Details screen. This screen allows for collecting specific information about the assessment including who was responsible, when it occurred, what sites or facilities were involved, and both descriptive and summary information. To use the Assessment Details screen, simply enter textual data into the fields provided. The figure below addresses the different parts of the Assessment Details screen.

The screenshot shows a form titled "Assessment Information" under the heading "Details". It contains four pairs of input fields:

- Assessment Name *: A text input field containing "My test assessment".
- Assessment Date: A date input field containing "9/24/2019".
- Facility Name: A text input field.
- City Or Site Name: A text input field.
- State/Province/Region: A text input field.

Figure: Assessment details screen

Assessment Name field: The Assessment Name text box is where the user enters the name of the assessment. The assessment name will also be displayed in the title area of the main CSET window and on the reports and will be used as the assessment file name if it isn't specifically changed by the user.

NOTE: An Assessment Name is required for CSET assessments. If the user hasn't provided one, CSET will name it "New Assessment".

Assessment datepicker: The Assessment Date-picker enables a user to add an initial date for the assessment. It requires a valid date format. Clicking the into the field will allow the user to select a date from a calendar control rather than entering the date manually.

Facility Name field: The Facility Name text box provides text input for identifying the name of the facility or facilities for which the assessment is created.

City/Site and State/Province/Region fields: The Location text boxes provide text input for identifying the name of the City or Site for which the assessment is created as well as the State, Province, or Region for which the assessment is created.

Note: Credit Union, Charter, and Asset fields will be available when using the Automated Cybersecurity Examination Toolkit.

Contacts Management

Contacts management is handled within the Assessment Details screen. Find the Assessment Contacts section underneath Assessment Name, Date, etc. to begin.

The screenshot shows a 'Contacts' panel. At the top, it displays 'Your Username' followed by 'Administrator'. To the right, it says 'Assessment Owner'. Below this, there is a button labeled '+ Add Contact'.

Figure: Contacts management panel

The Contacts panel shows first shows the assessment owner's name and below that will be their email address. This is the user who created the assessment.

To add a contact click the "Add Contact" button.

The screenshot shows a 'Adding a new contact' dialogue box. It includes fields for 'First Name' (with placeholder 'First Name'), 'Last Name' (with placeholder 'Last Name'), and 'Email' (with placeholder 'Email Address'). Below these is a 'Role' section with two options: 'User' (which is selected) and 'Administrator'. At the bottom are 'Save' and 'Cancel' buttons.

Figure: Adding a new contact

Add a New Contact: After selecting "Add Contact" a dialogue will open up below. Add the contacts information in the First Name, Last Name, and Email fields. If the contact has been previously associated with the user then the fields will auto-populate.

Select the User or Administrator role toggle. Administrators can add and remove contacts to an assessment, and delete assessments. There must be an Administrator assigned to an assessment at all times.

Select Save or Cancel to exit the dialogue.

When a user is added to an assessment they are sent an email inviting them to that CSET assessment. If they haven't yet registered for a CSET account they will be sent an additional email to walk them through the registration process.

Contacts

Your Username **Administrator** Assessment Owner

Test User
user@testing
User

Change Email Remove

+ Add Contact

Figure: Added user to assessment and contact icons



Editing a Contact: Clicking the Change icon makes the contact text field editable so that changes can be made. Click the save button to commit changes.



Emailing a Contact: Clicking the Email icon will open up an email dialogue so that users can customize their message.

✉ Invitation Email

From: Your Username

To:

Subject:

You have been invited to participate in a CSET assessment

Message:
You have been invited to participate in a CSET assessment.
Please log into your CSET account to participate. If you have not used CSET before, an account has been created for you, and a second email will be sent to this email address with instructions on logging in for the first time.

Send Cancel

Figure. Invitation email dialogue

For the individual email invitation CSET will fill in the "To" field with the contact information with the user in the field next to the icon. The user can customize the email and hit "Send".

Removing a Contact: Clicking the Remove icon  allows the user to delete contacts from an assessment. A confirmation dialogue will come up.

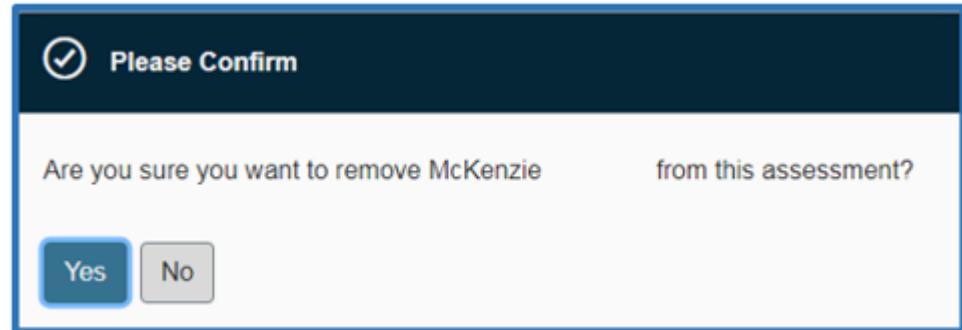


Figure. Contact deletion dialogue

Selecting "Yes" will remove the contact from the assessment. Selecting "No" will keep the user associated with the assessment.

Sector and Demographic Information Screen

The Sector and Demographics Information screen collects sector and demographic information about the assessment. Completing these fields allows the CSET tool to help the user identify the appropriate Standards and questions that will be asked on the assessment. The figure below describes the Sector and Demographic Information screen.

The screenshot shows a form titled "Demographics". It includes four dropdown menus:

- "Sector": A dropdown menu currently showing "Not Selected".
- "Industry": A dropdown menu currently showing "Small (1-2 hour) assessment".
- "What is the gross value of the asset you are trying to protect?": A dropdown menu currently showing "Not Selected".
- "What is the relative expected effort for this assessment?": A dropdown menu currently showing "Small (1-2 hour) assessment".

Figure: Sector and demographic information screen

Sector dropdown: The Sector dropdown list contains a list of industry sectors. Users should select the sector most relevant to their industry.

Industry dropdown: The Industry dropdown list provides a list of industries relevant to the selected Sector. Once the user selects a Sector, the Industry dropdown list will be populated with information relevant to the selected sector. Users should select the industry most relevant to their business.

Asset Gross Value dropdown: The Asset Gross Value dropdown allows the user to provide a rough dollar value estimate of the assets. CSET uses this information when determining the correct Standard to recommend to the user.

Relative Effort dropdown: The Relative Effort dropdown contains a list from small (1-2 hour) to 2 weeks for assessment time.

Security Assurance Level (SAL) Selection

The Security Assurance Level or SAL is a measure that determines the level of rigor applied to the assessment and also determines the number of questions required for the assessment. This section provides information on the Security Assurance Level or SAL process, the different types of SALs available in CSET, and the options for selecting the correct SAL for the current assessment.

Select from the SAL options below to learn more.

Simple SAL Selection

The Simple SAL selection window allows the user to quickly and easily select the Security Assurance Level for the assessment. This option is best for advanced users that know the appropriate SAL or CIA levels for their assessment and don't require assistance to determine the appropriate SAL. The figure below shows the Simple SAL selection screen.

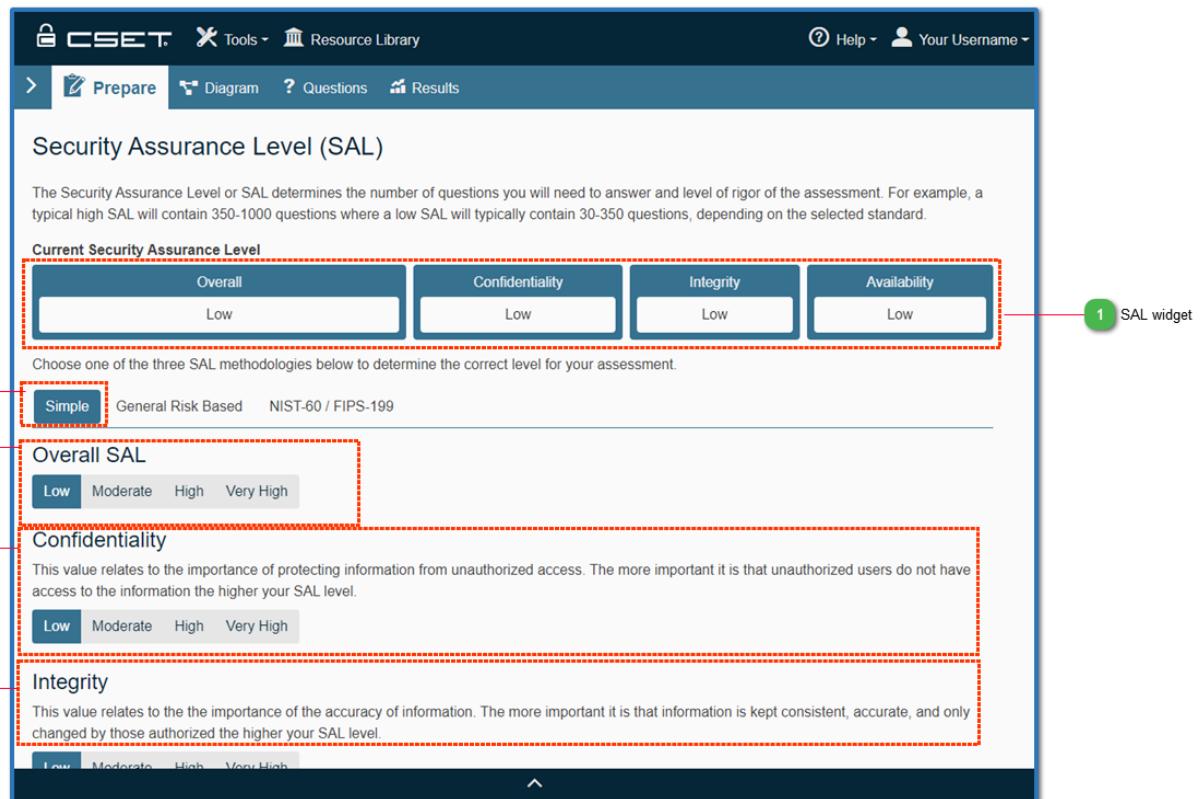


Figure: Standard SAL selection screen

1 SAL widget



The SAL Widget is a display-only image that indicates to the user how their SAL selections are affecting the Overall SAL and CIA scores.

2 Simple SAL button



The Simple SAL button is blue when selected. This indicates that the user is on the Simple SAL screen.

3 Overall SAL buttons

Overall SAL



The Overall SAL Selection buttons allow the user to quickly and easily select the Overall SAL for the assessment. Simply select the appropriate level and then click the "Next" button to navigate to the next screen. The selected SAL will be saved and associated with the assessment.

The default SAL is Low. The available levels include:

- Low
- Moderate
- High
- Very High

Low, Moderate, and High correspond with the levels identified by NIST in the NIST SP800-53 Standards, the NIST SP800-60 Volumes 1 and 2 documents, and the Chemical Facility Anti-Terrorism Standards (CFATS) risk-based tiering structure. Very High is defined in CSET as comprising all controls including all optional enhancements. It is used to accommodate the multiple Standards available in CSET.

The levels of potential impact are defined as:

Low: The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

Moderate: The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

High: The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Very High: A level of Very High is not defined in the NIST SP800-53 based Standards. It is included in CSET to accommodate the multiple Standards available in the tool and is defined as including all controls and all optional control enhancements.

4 Confidentiality SAL buttons

Confidentiality

This value relates to the importance of protecting information from unauthorized access. The more important it is that unauthorized users do not have access to the information the higher your SAL level.

Low Moderate High Very High

The Confidentiality SAL Selection buttons allow the user to select the appropriate Confidentiality level if it is known. The overall SAL will be determined based on the highest level selected between the selected Confidentiality, Integrity, and Availability levels.

5 Integrity SAL buttons

Integrity

This value relates to the the importance of the accuracy of information. The more important it is that information is kept consistent, accurate, and only changed by those authorized the higher your SAL level.

The Integrity SAL Selection buttons allow the user to select the appropriate Integrity level if it is known. The overall SAL will be determined based on the highest level selected between the selected Confidentiality, Integrity, and Availability levels.

Availability SAL buttons

(Not pictured) The Availability SAL Selection buttons allow the user to select the appropriate Availability level if it is known. The overall SAL will be determined based on the highest level selected between the selected Confidentiality, Integrity, and Availability levels.

Tip: CSET only uses one of the SAL types. The highest SAL rating out of all of them is what the user's assessment will be based on.

General SAL Selection

The General SAL Selection screen helps the user to determine the overall SAL for the assessment by selecting the potential impacts on people and economic factors in the event that systems are compromised. The General SAL Selection screen is described in the figure below.

The General SAL approach is consequence based. To use the screen, simply move the sliders to align with the total number of people or total dollar amount impacted for each question and category. Answers should be provided for both onsite and offsite impact.

For example, to determine the numeric value for potential injury, estimate the number of people, (onsite at the facility or those affected offsite) who could be injured without the need for hospitalization, should the scenario occur.

Estimate a worst-case number by assuming a full work shift with the addition of any visitors, contractors, vendors, etc., who may also be onsite. For the offsite estimate, assume peak occupancy of affected areas. For example, if a business district will be impacted by an event, then plan the estimate during the primary business hours. Consider all aspects of the scenario such as chain reactions. An explosion could be followed by a fire that could then close roadways, or even release toxic materials.

When considering the money-based questions, consider all costs including legal fees, fines, penalties, replacement costs, compensation, etc.

The Security Assurance Level (SAL) determines the number of questions you will need to answer and level of rigor of the assessment. For example, a typical high SAL will contain 350-1000 questions where a low SAL will typically contain 30-350 questions, depending on the selected standard.

Overall SAL widget (1)

Overall
Very High

General SAL button (2)

Choose one of the three SAL methodologies below to determine the correct level for your assessment.

Simple General Risk Based NIST-60 / FIPS-199

Overall SAL buttons (3)

Overall SAL
Low Moderate High Very High

Answer the following questions to help determine the SAL for your assessment by selecting the potential impacts on people and/or economic factors in the event your system is compromised.

If control systems were maliciously accessed and manipulated to cause harm, how many people could sustain injuries not requiring hospital stay in a worst-case scenario? (Consider injuries caused due to any reason.)

Onsite SAL slider (4)

On Site None injuries On Site > 1000 injuries

Offsite SAL slider (5)

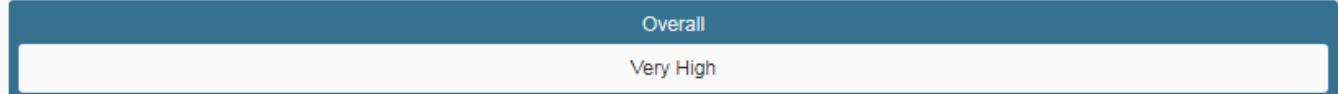
Off Site None injuries Off Site > 1000 injuries

SAL slider selector (6)

1-10 11-50 51-100 101-250 251-500 501-750 751-1000 > 1000

Figure: General SAL screen

1 Overall SAL widget



The SAL Widget is a display-only image that indicates to the user how their SAL selections are affecting the Overall SAL.

2 General SAL button

General Risk Based

The General SAL button is blue when selected. This indicates that the user is on the General SAL screen.

3 Overall SAL buttons

Overall SAL

Low Moderate High **Very High**

The Overall SAL Selection buttons allow the user to quickly and easily select the Overall SAL for the assessment. Simply select the appropriate level and then click the "Next" button to navigate to the next screen. The selected SAL will be saved and associated with the assessment.

The default SAL is Low. The available levels include:

- Low
- Moderate
- High
- Very High

Low, Moderate, and High correspond with the levels identified by NIST in the NIST SP800-53 Standards, the NIST SP800-60 Volumes 1 and 2 documents, and the Chemical Facility Anti-Terrorism Standards (CFATS) risk-based tiering structure. Very High is defined in CSET as comprising all controls including all optional enhancements. It is used to accommodate the multiple Standards available in CSET.

The levels of potential impact are defined as:

Low: The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

Moderate: The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

High: The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Very High: A level of Very High is not defined in the NIST SP800-53 based Standards. It is included in CSET to accommodate the multiple Standards available in the tool and is defined as including all controls and all optional control enhancements.

4 Onsite SAL slider



On-Site sliders indicate potential impacts to people or facilities that are on-site.

The user should estimate a worst-case number by assuming a full work shift with the addition of any visitors, contractors, vendors, etc., who may also be on site. All aspects of the scenario, such as chain reactions, should be considered. For example, an explosion could be followed by a fire that could then release toxic materials.

5 Offsite SAL slider



Off-Site sliders indicate potential impacts to people or facilities that are off site or in surrounding communities.

The user should estimate a worst-case number by assuming a maximum number of people present in the surrounding communities. All aspects of the scenario should be considered such as chain reactions. For example, an explosion could be followed by a fire which could then release toxic materials.

6 SAL slider selector



The SAL slider selector is used to indicate the correct value assigned to the question. The overall SAL is determined based on the values of all SAL slider selectors on the screen.

Tip: CSET only uses one of the SAL types. The highest SAL rating out of all of them is what the user's assessment will be based on.

General SAL – Injury

The slider bars provide a general range of values for both human and economic impact. The range of values is somewhat broad but allows for a uniform way of measuring the various categories. Review the question and move the slider to the best estimate of the answer.

Onsite

Estimate the number of onsite people who could be injured (without the need for hospitalization) should the scenario occur.

Estimate a worst-case number by assuming a full work shift with the addition of any visitors, contractors, vendors, etc., who may also be on site. Consider all aspects of the scenario such as chain reactions. For example, an explosion could be followed by a fire, which could then release toxic materials.

Offsite

Estimate the number of offsite people who could be injured (without the need for hospitalization) should the scenario occur.

Estimate a worst-case number by assuming a maximum number of people present in the surrounding communities. Consider all aspects of the scenario such as chain reactions. For example, an explosion could be followed by a fire, which could then release toxic materials.

General SAL – Hospital

The slider bars provide a general range of values for both human and economic impact. The range of values is somewhat broad but allows for a uniform way of measuring the various categories. Review the question and move the slider to the best estimate of the answer.

Onsite

Estimate the number of onsite people who could be injured and require hospitalization should the scenario occur.

Estimate a worst-case number by assuming a full work shift with the addition of any visitors, contractors, vendors, etc., who may also be on site. Consider all aspects of the scenario such as chain reactions. For example, an explosion could be followed by a fire, which could then release toxic materials.

Offsite

Estimate the number of offsite people who could be injured and require hospitalization should the scenario occur.

Estimate a worst-case number by assuming a maximum number of people present in the surrounding communities. Consider all aspects of the scenario such as chain reactions. For example, an explosion could be followed by a fire, which could then release toxic materials.

General SAL – Death

The slider bars provide a general range of values for both human and economic impact. The range of values is somewhat broad but allows for a uniform way of measuring the various categories. Review the question and move the slider to the best estimate of the answer.

Onsite

Estimate the number of onsite people who could be killed should the scenario occur.

Estimate a worst-case number by assuming a full work shift with the addition of any visitors, contractors, vendors, etc., who may also be on site. Consider all aspects of the scenario such as chain reactions. For example, an explosion could be followed by a fire, which could then release toxic materials.

Offsite

Estimate the number of offsite people who could be killed should the scenario occur.

Estimate a worst-case number by assuming a maximum number of people present in the surrounding communities. Consider all aspects of the scenario such as chain reactions. For example, an explosion could be followed by a fire, which could then release toxic materials.

General SAL – Capital Assets

The slider bars provide a general range of values for both human and economic impact. The range of values is somewhat broad but allows for a uniform way of measuring the various categories. Review the question and move the slider to the best estimate of the answer.

Onsite

Capital Assets are tangible property owned or used by the organization including buildings, structures, trailers, vehicles, machinery, utilities, office equipment, fixtures, furniture, and land.

Calculate the costs by multiplying the replacement cost of the asset by the estimated damage in percent.

Offsite

Capital Assets are tangible property used by the surrounding communities such as buildings, structures, vehicles, transit systems, roads, bridges, machinery, utilities, livestock, agricultural products, home and business equipment, fixtures, furniture, and land.

Calculate the costs by multiplying the replacement cost of the property by the estimated damage in percent.

General SAL – Economic Impact

The slider bars provide a general range of values for both human and economic impact. The range of values is somewhat broad but allows for a uniform way of measuring the various categories. Review the question and move the slider to the best estimate of the answer.

Onsite

Economic impact includes costs because of loss of production, damage or loss of product or feed stock, damage or loss of control system logic (damage to the physical system components should be counted under capital assets), damage or loss of data, costs of lawsuits, etc.

To estimate the cost of production loss, divide the annual budget by 365 (to calculate the daily budget) then multiply by the estimated down time in days. Include an estimate of displacement costs. That is, the estimated cost of working from an alternate, temporary location such as using a rented trailer for administrative functions. The cost of lawsuits with the associated loss of reputation is difficult to estimate. Look to history for the occurrence of similar scenarios for an indication of economic impact.

Offsite

Economic impact includes costs because of the communities' loss of supplies and services (food, power, water, medical services, etc.), loss of access to jobs, cost of emergency response actions, damage or destruction of agricultural land, etc.

Include an estimate of displacement costs for hospitals, schools, churches, and homes. The cost of lawsuits with the associated loss of reputation is difficult to estimate. Look to history for the occurrence of similar scenarios for an indication of economic impact.

General SAL – Environmental Cleanup

The slider bars provide a general range of values for both human and economic impact. The range of values is somewhat broad but allows for a uniform way of measuring the various categories. Review the question and move the slider to the best estimate of the answer.

Onsite

Estimate costs for direct and contract labor for cleanup and remediation, equipment, rentals, materials, waste disposal, permitting fees, investigation support, and fines.

Costs should be estimated for onsite impacts.

Offsite

Estimate costs for direct and contract labor for cleanup and remediation of surrounding communities, equipment, rentals, materials, waste disposal, permitting fees, investigation support, and fines.

Costs should be estimated for the impacts to (offsite) communities.

General SAL Considerations

The information here provides additional guidance for users in determining their General Security Assurance Level (SAL).

Characterize Assets

This step identifies assets that, if compromised, have the potential to cause undesirable consequences. In addition, assets owned by the organization or in proximity of the compromised facility that could be open to danger should be identified.

The options and resources in the following list may be used, as appropriate, for determining assets:

- Assets identified in risk and vulnerability assessments;
- Capacity, operation, management, and maintenance manuals;
- Risk management program manual;
- Hazardous waste operations and emergency response Standards;
- Emergency operations plan, particularly event-escalation criteria;
- Y2K documentation, including asset inventory, criticality determination, contingency plans, etc.;
- Asset inventory and criticality rating in the Computerized Maintenance Management System (CMMS);
- Inventory list of process control/SCADA hardware, including interfaces;
- Safety incident reports indicating accidents or near misses;
- Area maps showing schools, businesses, residential areas, rivers, or other transport paths;
- Population distributions; and
- Wind and water flow maps.

Define Worst-Case Scenarios

This step helps the assessment team acknowledge and consider the worst-case scenarios.

In defining worst-case scenarios, it is important to realize that many different ways are available to initiate a compromise of a control system. These include: (1) intentional, directed attacks with the intent of taking control of the system; (2) undirected attacks, such as viruses or worms, that can cause the system to malfunction; and (3) accidents that are caused by or result in inappropriate actions taken by an operator.

The worst-case scenarios should focus on the results, not the method, except as it relates to the compromise. In most cases, an undirected attack will cause problems, such as denial of service, which can shut down the control system and possibly prevent corrective action being taken. Directed attacks can result in an unauthorized person taking control of the system, and then opening or closing valves to create dangerous mixtures or release of materials to the environment.

The secondary consequences of a system compromise should also be considered in developing scenarios. For example, the loss of a power grid supplying power to a large population area may cause a domino effect of further power loss to financial centers, businesses, transportation systems, and heating, cooling for homes, hospitals, schools, etc.

An example of a worst-case scenario might be the intentional and undetected opening of one or more valves causing the release of a toxic material to the atmosphere. The material could then be carried over to a nearby community resulting in injuries, fines, and environmental cleanup costs.

Estimate Consequences

Ask these questions. If the identified scenarios were to occur, what would the consequences be to the organization including its customers and the surrounding community? How would the organization be impacted by the following?

- Personal health and safety (injury, loss of life);
- Loss of capital assets;
- Adverse environmental impacts; and
- Adverse economic impacts.

The guidelines in this section are provided to assist in estimating a value for the consequences of an undesired event. The guidelines are not prescriptive and do not replace current consequence estimating procedures that the organization may have in place. Each guideline presented in this section correlates to categories contained in questions to determine the SAL for both onsite and distributed assets.

Remember, for a worst-case scenario, select worst-case conditions.

Injury and Loss-of-Life Estimate

Estimates for injury and loss of life can be challenging to determine. To estimate the number of people at risk for each scenario, consider the agents that would cause injury or death, their impact area, and the method of transport. Also, there may be several different agents for a single scenario, such as the force of an explosion, a subsequent fire, and the release of toxic materials.

The tool divides affected persons into two groups: personnel that are onsite and people that are outside the facility boundaries (i.e., people in the surrounding communities). Start by counting the number of people most likely to be onsite or in the area of the distributed asset, and then estimate the number of people outside the facility boundaries that could be affected. Different times of the day or different environmental conditions could exacerbate the situation.

The tool also breaks injuries into two categories: injuries that do not require hospital stay and injuries that do require hospital stay. For example, minor exposures to contaminants that can be treated with an eyewash or shower are not as serious as those requiring hospitalization because of a more serious exposure.

Capital Asset Loss Estimate

Capital assets are tangible property used by the organization or community such as buildings, machinery, fixtures, furniture, and equipment.

To estimate the organizational capital asset loss, perform the following steps:

- Determine the total estimated value of each potentially impacted site or distributed asset for each example scenario. The following is a typical list of asset types to consider:
 - Buildings, including all structures that serve as buildings such as permanently established trailers.
 - Machinery and equipment, including all motor vehicles (licensed and nonlicensed), trailers, construction and maintenance equipment, fixtures, computers, and office furniture.
- Estimated structure losses (structure replacement value multiplied by the estimated damage in percent). For example, if a plant's structure replacement value equals \$100,000, and the expected damage is 40 percent of the structure, then the loss to this structure is \$40,000.
- Estimated content losses (content replacement value multiplied by the estimated damage in percent). For example, if the plant's content replacement value equals \$225,000, and the expected damage is 10 percent of the contents, then the losses to these contents are \$22,500.
- Structure and content loss are calculated as

For each asset,

$$\text{Structure loss (\$)} = (\text{structure replacement value}(\$)) \times (\% \text{ damage})$$

$$\text{Contents loss (\$)} = (\text{contents replacement value (\$)}) \times (\% \text{ damage})$$

To estimate the community capital asset loss,

- Estimate the value of capital assets that are within the impact area of the scenario and the estimated extent of damage to these capital assets. The same process described for determining organizational assets can be used for determining community assets.

Environmental Impacts

Impacts to the environment can be wide ranging and have far-reaching consequences. These consequences may include cleanup, as a minimum, remediation, and investigations with fines from regulatory agencies. Calculate the environmental consequence by estimating costs for the following:

- Direct labor (for cleanup, remediation, etc.);
- Contractor (for cleanup, remediation, etc.);
- Equipment;
- Rented equipment;
- Materials;
- Fees for permits;
- Community mitigation efforts (e.g., portable toilets);
- Investigation support;
- Fines; and
- Material disposal.

Economic Impact

The economic impact because of a worst-case scenario may include costs associated with loss of production, impact to reputation, damage or loss of finished product or feed stock, damage to or loss of the control system because of cyber damage requiring reprogramming of machines or rewriting of code, damage to the physical control hardware would be included under capital equipment, corrective action to prevent similar intrusions in the future, possible law suits, etc.

Losses associated with production are much easier to estimate than some other impacts. Production losses can be estimated using the following recommendations:

- Determine functional downtime or the time (in days) that the function would be disrupted because of the event.
- Estimate the average number of days various functions might be unavailable following a worst-case scenario occurrence.
- Estimate the daily cost of the functional downtime. Divide the average annual budget by 365 to determine the average daily operating budget or sales. Multiply the average daily operating budget by the functional downtime to determine the cost of the loss of function for the period that the service was unable to operate because of the event. For example, if a plant has an annual budget of \$6,000,000 and an average daily budget of \$16,438 (\$6,000,000/365), the losses could be estimated by using the annual budget as a proxy for the value of the service to the community. For example, if the plant were down for 7 days, then the cost for the loss of use for 7 days would be \$115,066 (\$16,438×7).
- Determine the displacement time, or the time in days, that a function may need to operate from a temporary location, if applicable. For example, if the administration building is inaccessible for 7 days (functional downtime) and operations are resumed from a trailer for the next 90 days, then the displacement time would be 90 days. Not all functions would require displacement before resuming operation.
- Multiply the displacement cost by the displacement time to determine the cost of the displacement from the regular place of business, as:

$$\begin{aligned} \text{For each asset, structure use and function loss} = \\ (\text{average daily operating budget (\$)}) \times (\text{functional downtime (# of days)}) + \\ (\text{displacement cost per day (\$)}) \times (\text{displacement time (# of days)}) \end{aligned}$$

Loss of finished product and feed stock can be estimated by using historical accounts of the amount of product kept onsite at any time. This may be either a maximum (worst case) or an average amount. The cost of the feed stock would be the replacement cost. If not having the feed stock on hand impacts the ability to restart the system, this would also affect loss of production. The loss of finished product would be the cost of producing the lost amount of the finished product. This could be determined by using production history as well.

The cost of cyber damage to the control system must be estimated based on what is most likely to be affected according to the scenario. The scenario may require the control system software to be rebuilt or the control code to be reworked, or it may require that an antivirus program be run on the system. The cost of this effort needs to be estimated. It may also require investigation of what caused the problem and the costs of reworking the system in order to implement a fix.

The economic impact because of loss of reputation or lawsuits is much harder to estimate. History of similar incidents either within the organization or within similar organizations might provide an indication of the potential economic impact.

EVALUATE TOTAL IMPACT

After evaluating each of the consequences and their costs, determine if areas are either counted twice or might mitigate or enhance the impact of the individual consequences. These may need to be adjusted. With these final figures, answer the questions for determining the SAL.

FIPS 199 SAL Selection

After clicking the FIPS 199 SAL Determination link on the top pill navigation of the SAL screen, the display will change to that shown in the figure below. This Instructions page provides links to a guide and the source documents.

The process is based on the Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* and the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*. These Standards apply to information within the US federal government and federal information systems.

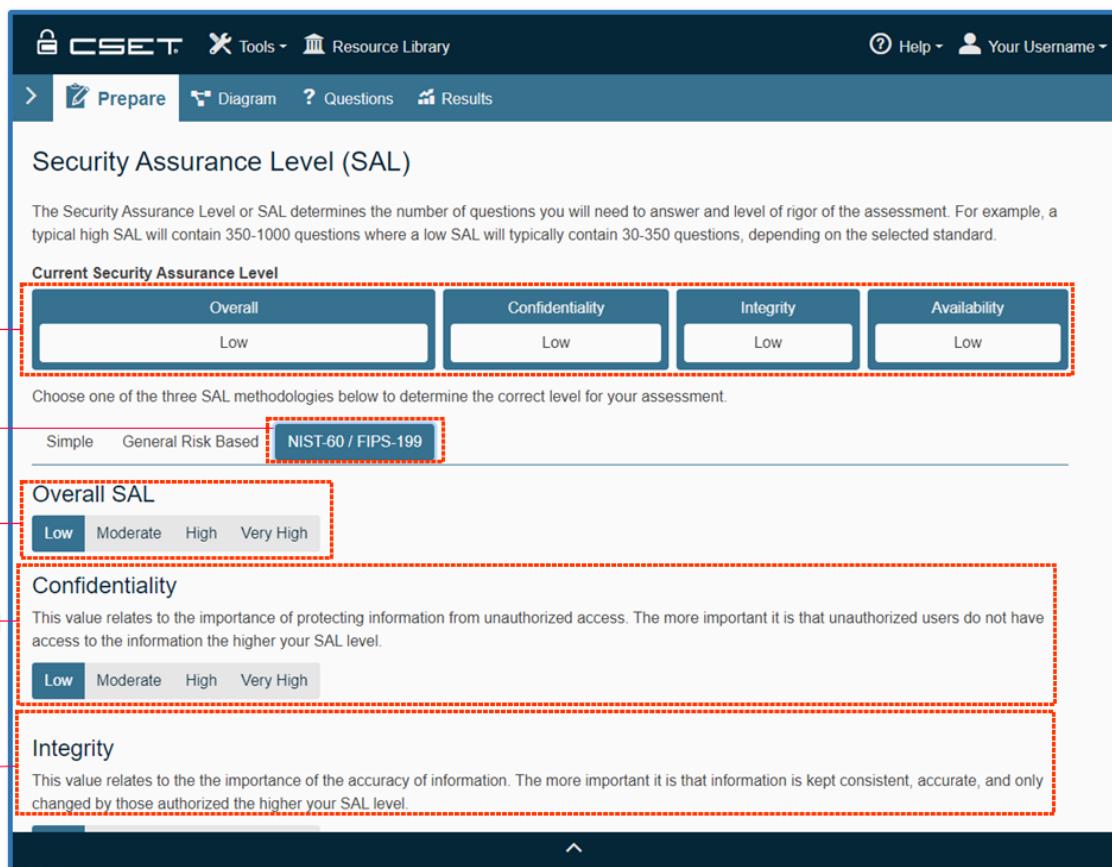


Figure: FIPS 199 SAL screen

1 Overall SAL widget

Overall Low	Confidentiality Low	Integrity Low	Availability Low
----------------	------------------------	------------------	---------------------

The SAL Widget is a display only image that indicates to the user how their SAL selections are affecting the Overall SAL.

2 NIST/FIPS SAL button

NIST-60 / FIPS-199

The NIST-60/FIPS-199 SAL button is blue when selected. This indicates that the user is on the NIST/FIPS SAL screen.

3

Overall SAL buttons

Overall SAL

Low **Moderate** **High** **Very High**

The Overall SAL Selection buttons allow the user to quickly and easily select the Overall SAL for the assessment. Simply select the appropriate level and then click the "Next" button to navigate to the next screen. The selected SAL will be saved and associated with the assessment.

The default SAL is Low. The available levels include:

- Low
- Moderate
- High
- Very High

Low, Moderate, and High correspond with the levels identified by NIST in the NIST SP800-53 Standards, the NIST SP800-60 Volumes 1 and 2 documents, and the Chemical Facility Anti-Terrorism Standards (CFATS) risk-based tiering structure. Very High is defined in CSET as comprising all controls including all optional enhancements. It is used to accommodate the multiple Standards available in CSET.

The levels of potential impact are defined as:

Low: The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

Moderate: The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

High: The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Very High: A level of Very High is not defined in the NIST SP800-53 based Standards. It is included in CSET to accommodate the multiple Standards available in the tool and is defined as including all controls and all optional control enhancements.

4

Confidentiality SAL buttons

Confidentiality

This value relates to the importance of protecting information from unauthorized access. The more important it is that unauthorized users do not have access to the information the higher your SAL level.

Low **Moderate** **High** **Very High**

The Confidentiality SAL Selection buttons allow the user to select the appropriate Confidentiality level if it is known. The overall SAL will be determined based on the highest level selected between the selected Confidentiality, Integrity, and Availability levels.

5

Integrity SAL buttons

Integrity

This value relates to the the importance of the accuracy of information. The more important it is that information is kept consistent, accurate, and only changed by those authorized the higher your SAL level.

The Integrity SAL Selection buttons allow the user to select the appropriate Integrity level if it is known. The overall SAL will be determined based on the highest level selected between the selected Confidentiality,

Integrity, and Availability levels.

Availability SAL buttons

(Not pictured) The Availability SAL Selection buttons allow the user to select the appropriate Availability level if it is known. The overall SAL will be determined based on the highest level selected between the selected Confidentiality, Integrity, and Availability levels.

Select Information Types: After selecting your SAL levels, the next step is to check all applicable information types.

CIA Values Based on Selected Information Types

Check applicable information types.

Type	C	I	A
<input type="checkbox"/> Air Transportation : D.11.3	LOW	LOW	LOW
<input type="checkbox"/> Asset and Liability Management : C.3.2.1	LOW	LOW	LOW
<input type="checkbox"/> Budget Execution : C.2.3.5	LOW	LOW	LOW
<input type="checkbox"/> Budget Formulation : C.2.3.1	LOW	LOW	LOW
<input type="checkbox"/> Budgeting & Performance Integration : C.2.3.8	LOW	LOW	LOW
<input type="checkbox"/> Capital Planning : C.2.3.2	LOW	LOW	LOW
<input type="checkbox"/> Collections & Receivables : C.3.2.6	LOW	MOD	LOW
<input type="checkbox"/> Contingency Planning : C.2.4.1	MOD	MOD	MOD

Figure: Selected information types tab

When an information type is selected in the list on the left of the screen, CSET displays that type with the values in the block on the right and at the same time dynamically updates the combined values in the block on the top, including the overall SAL.

No specific definition is given for each information type in CSET. To understand how the types are broken out the guidance documents discussed above must be opened.

Answer Questions: The next step in determining the SAL using the FIPS 199 method is to answer a short set of questions that may adjust the level in one or more of the categories. The figure below shows the screen when the Answer Questions tab has been clicked.

Answer Questions

Does aggregation of information on this system reveal sensitive patterns and plans, or facilitate access to sensitive or critical systems?

Yes No

Does/could access to this system result in some form of access to other more sensitive or critical systems (e.g., over a network)?

Yes No

Are there extenuating circumstances such as: The system provides critical process flow or security capability, the public visibility of the system, the sheer number of other systems reliant on its operation, or the overall cost of the systems replacement?

Yes No

Would unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) adversely affect operations or seriously damage mission function and/or public confidence?

Yes No

Would either physical or logical destruction of the system result in very large expenditures to restore the system and/or require a long period of time for recovery?

Yes No

Figure: Answer Questions

After the Answer Questions section is opened, CSET will display a set of eight questions that were taken from the NIST documents. The answers to these questions may cause the SAL values to be changed. As the user marks either Yes or No to the question, CSET will dynamically update the Adjusted for System Questions fields at the top of the screen. The SAL will affect how many questions must be answered in both the Questions and Standard Requirements modes.

Determine Special Factors: The final step is to determine the Special Factors. They come from NIST SP800-60, Volume II and are exceptions to the provisional impact assignments of Low, Medium, and High for the selected information type. To add the Special Factors text to the SAL Values, click the security objective value assignment for that information type. Not all information types are associated with Special Factors. Those that are associated with Special Factors have a blue text color (Seen in Figure Checkboxes). Clicking the link will enter that Special Factors text into the field shown Figure. Determine Special Factors.

For example, selecting Air Transportation results in the Confidentiality value of Low, which is seen in blue. Clicking the word Low enters the Special Factor text into the block at the bottom of the screen. This text is fully editable.

Determine Special Factors

Confidentiality Special Factor

Special Factors Affecting Confidentiality Impact Determination: Unauthorized disclosure of information (e.g., investigations, maintenance) that has not been adequately researched, coordinated, or edited can result in serious economic harm to individuals and to corporations. Loss in public confidence is a further

Integrity Special Factor

Availability Special Factor

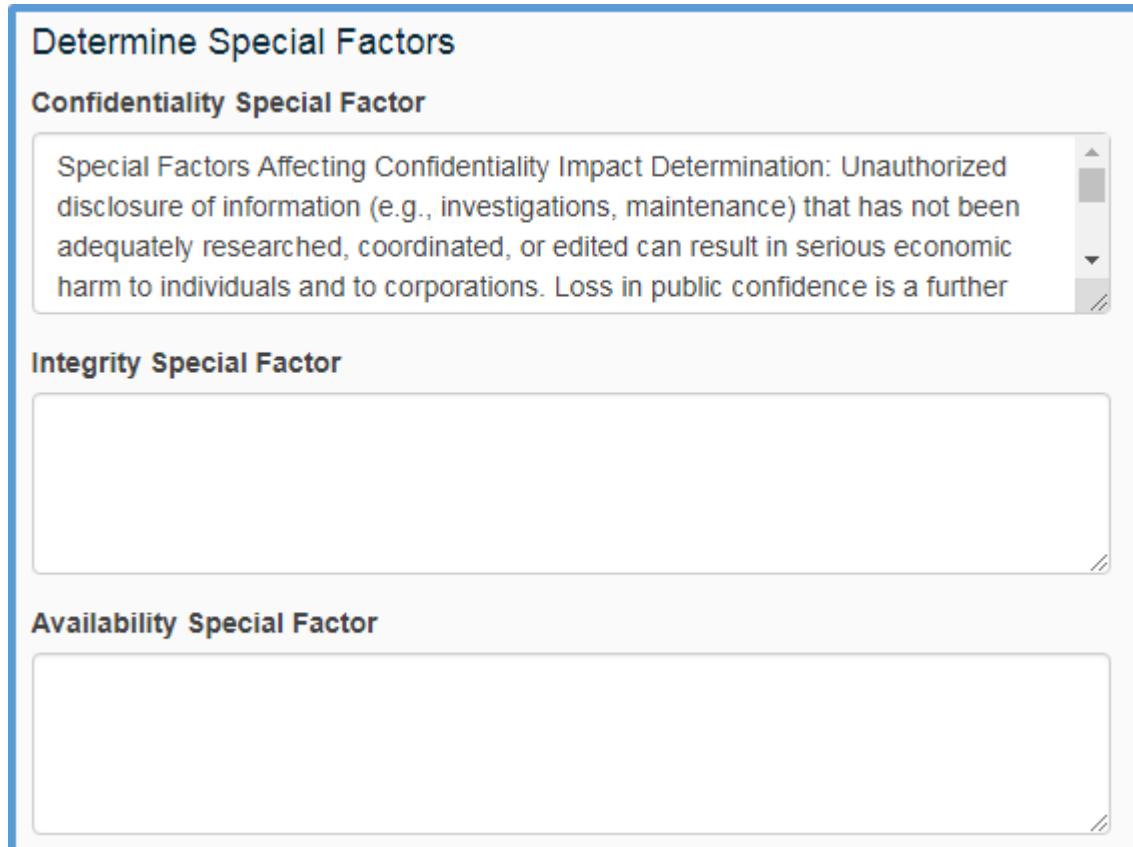


Figure: Determine Special Factors

If another information type is checked and the Special Factor text is entered into the block for the same security objective, the previous text in the Special Factors text areas will be overwritten. A warning message, similar to that shown in the figure below, will be shown to confirm that the text is to be overwritten. Only one Special Factor may be used for each security objective.

This will overwrite the current Confidentiality special factor text. Do you want to continue?

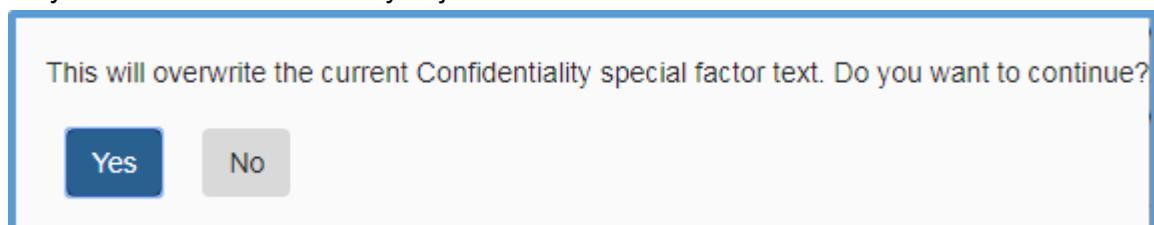


Figure: Special factors overwrite warning

Tip: CSET only uses one of the SAL types. The highest SAL rating out of all of them is what the user's assessment will be based on.

Cybersecurity Standard Selection

This section provides information on understanding the Standards and requirements available in CSET. The figure below describes the Cybersecurity Standard Selection screen.

CSET Standards are defined on the [CSET Standards and Groupings](#) page.

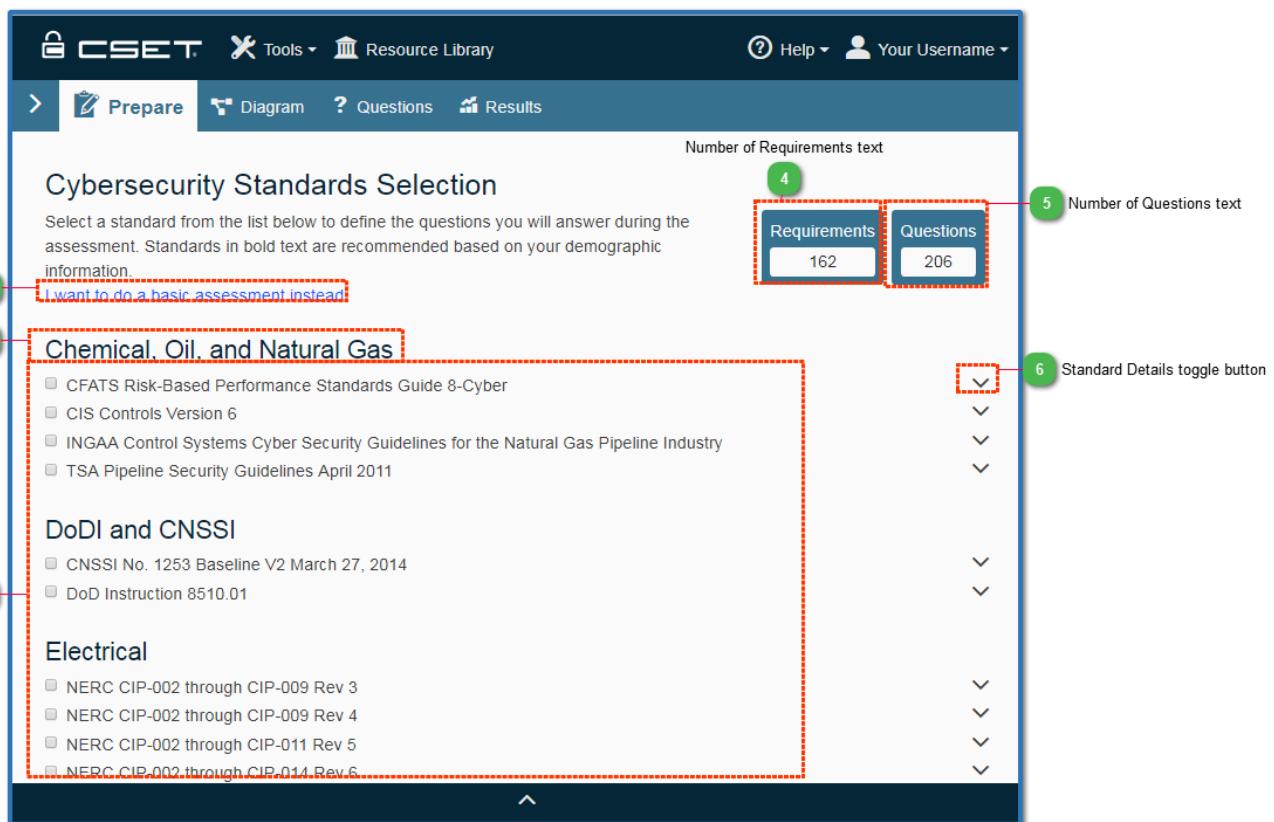


Figure: Cybersecurity Standard Selection screen

1 Basic Mode option

[I want to do a basic assessment instead](#)

Selecting the Basic Mode option will cause the CSET tool to build the assessment questions based on the sector, demographic and other information selected during the preparation process. A knowledge of cybersecurity Standards is not required for the Basic Mode option.

2 Standard Group text

Chemical, Oil, and Natural Gas

The Standard Group text shows the group to which a specific Standard belongs. The Standard List is sorted by the Group to help the user more easily find specific Standards within a group.

3 Standards list

- CFATS Risk-Based Performance Standards Guide 8-Cyber
- CIS Controls Version 6
- INGAA Control Systems Cyber Security Guidelines for the Natural Gas Pipeline Industry
- TSA Pipeline Security Guidelines April 2011

DoDI and CNSSI

- CNSSI No. 1253 Baseline V2 March 27, 2014
- DoD Instruction 8510.01

Electrical

- NERC CIP-002 through CIP-009 Rev 3
- NERC CIP-002 through CIP-009 Rev 4
- NERC CIP-002 through CIP-011 Rev 5
- NERC CIP-002 through CIP-014 Rev 6

The Standards list displays a list of all available Standards on which the assessment questions may be based. Some standards will be recommended based on demographic information indicated by the user (shown in bold). Some Standards are only available in "Requirements Mode" and may be disabled based on the assessment mode previously selected. Standards are organized into Groups and can be sorted accordingly. Each Standard also has details or descriptions to help the user better identify the Standard.

Any Custom Questionnaires associated with the installation of CSET will also be available on the Standard List.

This is where the unlocked Standards from [Enable Protected Features](#) will be shown.

4

Number of Requirements text

Requirements

162

The Number of Requirements text will update as Standards are selected and provides an indication to the user how large the assessment will be.

5

Number of Questions text

Questions

206

The Number of Questions text will update as Standards are selected and provides an indication to the user how large the assessment will be.

6

Standard Details toggle button



The Standard Details toggle button will toggle between showing and hiding descriptions of the selected Standard to help the user better understand what the Standards contain.

CSET Standards and Groupings

This page describes the Cybersecurity Standards used by the CSET tool. Standards are grouped into multiple areas as explained below.

Chemical, Oil, and Natural Gas

Critical Security Controls Version 6: The Center for Internet Security (CIS) presents the CIS Controls for Effective Cyber Defense Version 6.0, a recommended set of actions that provide specific and actionable ways to stop today's most pervasive and dangerous cyber attacks. The CIS Controls are especially relevant because they are updated by cyber experts based on actual attack data pulled from a variety of public and private threat sources. Version 6 incorporates recommended changes from the cybersecurity community to reflect the latest technologies and threats. The new Controls include a new Control for "Email and Web Browser Protections," a deleted Control on "Secure Network Engineering," and a re-ordering to make "Controlled Use of Administration Privileges" higher in priority. This version also includes a new metrics companion guide.

CFATS Risk-Based Performance Standards Guide 8–Cyber: This Standards guidance is part of the overall efforts defined in 6 Code of Federal Regulations (CFR) Part 27 to protect chemical facilities from the effects of a terrorist attack. CFATS, or the Chemical Facilities Anti-Terrorism Standards, is made up of 18 Risk-Based Performance Standards Guidance (RBPS) sections that provide guidance on protecting various aspects of a chemical facility. RBPS 8 is focused on cybersecurity with emphasis on protecting both information management and control system-based networks. It is the only RBPS that is pertinent to the CSET.

The audience for this instruction is personnel involved in the chemical industry who are required to comply with the 6 CFR Part 27 as well as others seeking to follow these simple actions to better protect their systems.

DHS has developed a risk-based tiering structure that will allow it to focus resources on the high-risk chemical facilities. To that end, DHS will assign facilities to one of four risk-based tiers ranging from very high (Tier 1) to low (Tier 4) risk. These tiers are unrelated to the Framework tiers.

INGAA Control Systems Cyber Security Guidelines for the Gas Pipeline Industry:

The Interstate Natural Gas Association of America (INGAA) is a trade organization for the natural gas pipeline industry in North America. As such, its Standard applies to the gas pipeline industry. The guidelines can be thought of as a subset of the Transportation Security Administration (TSA) Pipeline Security Guidelines and focus on securing large supervisory control and data acquisition (SCADA) systems and smaller, local control systems. The intended audience is administrators, network security personnel, SCADA software manufacturers, operators, vendors, and other stakeholders involved in the natural gas pipeline industry. Because INGAA is a non-government body, a disclaimer will be seen upon selection of this Standard.

DODI and CNSSI:

CNSSI No. 1253 Baseline, V2 March 27, 2014: This update was released in March of 2014 and supersedes the older CNSSI No. 1253 Baseline listed earlier. The intent and purpose of the Standard is the same as described above. Use this version for new assessments.

DoD Instruction 8500.2: This DoD Instruction, Information Assurance (IA) Implementation, implements policy, assigns responsibilities, and prescribes procedures for applying integrated, layered protection to DoD information systems and networks. It is applicable to information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of U.S. military-related information. It is predicated on five competencies, the ability to: (1) assess security needs and capabilities, (2) develop a purposeful security design or configuration, (3) implement required controls or safeguards, (4) test and verify, and (5) manage changes to an established baseline in a secure manner. The audience for this instruction is personnel who use IT to share DoD information across the Global Information Grid.

DoD Instruction 8510.01: Risk Management Framework (RMF) for DoD IT applies to all DoD IT that receives, processes, stores, displays, or transmits DoD information. The instruction implements NIST SP 800-37 and re-designates the DIACAP Technical Advisory Group (TAG) as the RMF TAG. The instruction also provides procedural guidance for the reciprocal acceptance of authorization decisions and artifacts within DoD, and between DoD and other federal agencies, for the authorization and connection of information systems. It uses controls from CNSSI 1253 V2 plus NIST SP800-53 Appendix J.

Electrical:

NERC CIP-002 through CIP-009, Rev. 3: The North American Electric Reliability Council (NERC) Critical Infrastructure Protection (CIP) Standards apply to the electric power industry. Standards CIP-002 through CIP-009 provide a cybersecurity framework (unrelated to the cybersecurity framework based Assessment Mode option) for the identification and protection of critical cyber assets to support reliable operation of the bulk electric system.

Standard CIP-002-3 requires the identification and documentation of the critical cyber assets. Standard CIP-003-3 requires that responsible entities have minimum security management controls in place to protect critical cyber assets. Standard CIP-004-3 requires that personnel having authorized cyber or authorized unescorted physical access to critical cyber assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-005-3 requires the identification and protection of the electronic security perimeters. Standard CIP-006-3 is intended to ensure the implementation of a physical security program. Standard CIP-007-3 requires responsible entities to define methods, processes, and procedures for securing those systems determined to be critical cyber assets. Standard CIP-008-3 ensures the identification, classification, response, and reporting of cybersecurity incidents; and Standard CIP-009-3 ensures that recovery plans are put in place.

The NERC CIP Standards are designed specifically for the needs of the electric power sector.

NERC CIP-002 through CIP-009, Rev. 4: Revision 4 of the CIP Standards has the same aims and audience as Revision 3. This version includes all the requirements that have been added or modified for Revision 4.

NERC CIP-002 through CIP-011, Rev. 5: Revision 5 of the CIP Standards has the same aims and audience as Versions 3 and 4. It does, however, include two additional sections. CIP-010 deals with configuration change management and vulnerability assessments. CIP-011 is concerned with information protection. This version includes all the requirements that have been added or modified for Revision 5.

NERC CIP-002 through CIP-011, Rev. 6: NERC CIP v6 is largely about scope, and so its impact will be dependent on how the scope expansion affects your organization. The expansion of requirements to low impact assets has zero impact if you don't have any. The same goes for the transient assets and removable media. While there aren't many organizations in that situation, scope reduction is absolutely a valid strategy for any compliance program, NERC CIP compliance included. While it may seem obvious to state, don't wait to determine how you're going to address the updated NERC CIP standards. If there's the potential for budgetary impact (and there is), the sooner you start planning, the better.

NISTIR 7628 Guidelines for Smart Grid Cyber Security, Vol 1: Dealing with Standards for the national electrical transmission systems and applicable to the electric sector, this National Institute of Standards and Technology (NIST) Interagency Report (IR) presents a framework that organizations can use to develop cybersecurity strategies to secure existing systems while upgrading to newer, smart grid technology. NISTIR includes identification of security requirements, risk assessment processes, and high-level architecture. It presents a sample logical interface reference model used to identify and define 22 logical interface categories within and across seven commonly accepted Smart Grid domains. The intended audience is individuals and organizations responsible for addressing cybersecurity for Smart Grid systems and the constituent subsystems of hardware and software components.

NISTIR 7628 Guidelines for Smart Grid Cyber Security, Vol 1 Rev. 1: Revision 1 of the NISTIR 7628 Guideline has the same aims and audience as the earlier version, but with updated information on Smart Grid technologies and implementations.

Financial:

ACET Maturity Assessment: Called the Automated Cybersecurity Examination Toolbox (ACET), it provides us with a repeatable, measurable and transparent process that improves and standardizes our supervision related to cybersecurity in all federally insured credit unions.

Payment Card Industry (PCI) Data Security Standard: The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect account data. PCI DSS applies to all entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers. PCI DSS also applies to all other entities that store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD).

General:

Catalog of Recommendations, Rev. 7: The Catalog of Recommendations or CoR questionnaires are based on the Catalog of Control Systems Security, Recommendations for Standards Developers. Development was initially sponsored by DHS with input from NIST and five national laboratories. Its original intent was to serve as a source of requirements and controls for the developers of ICS Standards. The CoR consolidated the requirements from 15 control system and information technology Standards. Version 7 is the latest version and incorporates changes and updates made in 2010.

The controls in the CoR are organized into families based on NIST SP800-53 with contributions from AGA, ISO, IEC, IEEE, ISA, NERC, and other Standards documents. Requirements for each security control include: (1) detailed recommended security practices and mechanisms, (2) supplemental guidance with information that may be beneficial for understanding and implementing the recommendations, and (3) requirement enhancements including supplementary security constraints for the recommendations.

The CoR is not limited for use by a specific industry sector. It is intended to be broad enough to provide any industry using control systems the flexibility needed to develop sound cybersecurity Standards specific to their individual security needs. Its use is strongly recommended if using the Standards-based approach.

Control Correlation Identifier Specification V2 release 0.1: One of the more recent information security innovations is the Control Correlation Identifier, or CCI. Each CCI provides a standard identifier and description for "singular, actionable statements" that comprise a security control or security best practice. The purpose of CCIs is to allow a high level statement made in a policy document (i.e., a security control) to be "decomposed" and explicitly associated with the low-level security settings that must be assessed to determine compliance with the objectives of that specific statement. Under the leadership of the Defense Information Systems Agency (DISA), a working group has been cataloging CCIs for the past several years. The collection has now been developed to the point that every assessment objective in the NIST SP 800-53A has been mapped to an individual CCI. The current list of CCIs can be downloaded in XML format (viewable in a web browser such as Internet Explorer). The URL for downloading is: <http://iase.disa.mil/stigs/cci/Pages/index.aspx>. DISA encourages feedback from the information security community; a comment form is provided for that purpose. DISA is also in the process of revising numerous Security Technical Implementation Guides (STIGs) to include references to CCIs that correspond to each of the recommended configuration settings.

Cybersecurity Capability Maturity Model (C2M2): The C2M2 is designed to be used by any organization to enhance its own cybersecurity capabilities. It focuses on the implementation and management of cybersecurity practices associated with the operation and use of information technology and operational technology assets and the environments in which they operate. The goal is to measure the maturity of an organization's cybersecurity capabilities and support ongoing development within an organization. To do so, it uses a system of Maturity Indicator Levels (MILs) applied to each of ten key domains such as Risk Management and Configuration Management.

MIL 0 is the lowest of the maturity models and is defined as Incomplete. Many organizations can achieve MIL 0 using an ad hoc approach. MIL 1 is Initiated, MIL 2 is Performed, and MIL 3, the highest maturity level, is Managed.

Also available are sector-specific C2M2s for Electricity, and Oil and Natural Gas that include the core C2M2 as well as additional reference material and implementation guidance specifically tailored for the referenced sector.

NIST Special Publication 800-171: This publication provides federal agencies with recommended requirements for protecting the confidentiality of Controlled Unclassified Information (CUI): (i) when the CUI is resident in nonfederal information systems and organizations; (ii) when the information systems where the CUI resides are not used or operated by contractors of federal agencies or other organizations on behalf of those agencies; and (iii) where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or government-wide policy for the CUI category or subcategory listed in the CUI Registry. The requirements apply to all components of nonfederal information systems and organizations that process, store, or transmit CUI, or provide security protection for such components.

NIST Special Publication 800-171 Rev. 1: The protection of Controlled Unclassified Information (CUI) resident in nonfederal systems and organizations is of paramount importance to federal agencies and can directly impact the ability of the federal government to successfully conduct its assigned missions and business operations. This publication provides federal agencies with a set of recommended security requirements for protecting the confidentiality of CUI when such information is resident in nonfederal systems and organizations; when the nonfederal organization is not collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency; and where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category or subcategory listed in the CUI Registry. The security requirements apply to all components of nonfederal systems and organizations that process, store, or transmit CUI, or that provide security protection for such components. The requirements are intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations.

Health Care:

Health Insurance Portability and Accountability Act Security Rule:

The Health Insurance Portability and Accountability Act of 1996 (HIPAA; Pub.L. 104–191, 110 Stat. 1936, enacted August 21, 1996) was enacted by the United States Congress and signed by President Bill Clinton in 1996. It has been known as the Kennedy–Kassebaum Act or Kassebaum–Kennedy Act after two of its leading sponsors.^{[1][2]} Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs. Title II of HIPAA, known as the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. Technical Safeguards – controlling access to computer systems and enabling covered entities to protect communications containing PHI transmitted electronically over open networks from being intercepted by anyone other than the intended recipient. Information systems housing PHI must be protected from intrusion. When information flows over open networks, some form of encryption must be used. If closed systems or networks are used, existing access controls are considered sufficient and encryption is optional. Each covered entity is responsible for ensuring that the data within its systems have not been changed or erased in an unauthorized manner. Data corroboration, including the use of check sum, double-keying, message authentication, and digital signature may be used to ensure data integrity. Covered entities must also authenticate entities with which they communicate. Authentication consists of corroborating that an entity is who it claims to be. Examples of corroboration include: password systems, two or three-way handshakes, telephone callback, and token systems. Covered entities must make documentation of their HIPAA practices available to the government to determine compliance. In addition to policies and procedures and access records, information technology documentation should also include a written record of all configuration settings on the components of the network because these components are complex, configurable, and always changing. Documented risk analysis and risk management programs are required. Covered entities must carefully consider the risks of their operations as they implement systems to comply with the act. (The requirement of risk analysis and risk management implies that the act's security requirements are a minimum standard and places responsibility on covered entities to take all reasonable precautions necessary to prevent PHI from being used for non health purposes.)

Information Technology:

The National Institute of Standards and Technology (NIST), Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems and Organizations, is the primary U.S. government Standard for securing information systems. Because many non federal entities have adopted its use, it is probably the most widely used Standard for IT system security.

NIST Special Publication 800-53, Rev. 3: The NIST SP800-53 provides guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the U.S. federal government. The guidelines apply to all components of an information system that process, store, or transmit federal information. Information system components can include mainframes, servers, workstations, operating systems, and applications. Network components can include firewalls, switches, routers, wireless access points, and network appliances. Servers can include database servers, authentication servers, electronic mail and web servers, proxy servers, and domain name servers. Information system components may be purchased commercially off-the-shelf or custom developed.

Although developed for the federal government, other organizations are encouraged to use the guidelines. In CSET, this version of the Standard does not include the adjustments addressed in Appendix I. See NIST SP800-53, Rev. 3 with Appendix I for those modified controls.

NIST Special Publication 800-53, Rev. 4: Revision 4 has the same audience and intended use as Revision 3; however, it includes updates, additions, and changes to make it more current and relevant. In CSET, Appendix I is separate.

NIST Special Publication 800-53, Rev. 4 App J: Appendix J of 800-53, Rev. 4, is titled the Privacy Control Catalog. It relates specifically to protection of individuals' privacy and their personally identifiable information (PII). The appendix provides a structured set of controls for protecting privacy and serves as a

roadmap for organizations to use in identifying and implementing privacy controls concerning the entire life cycle of PII.

NIST Special Publication 800-53, Rev. 5: This update to NIST Special Publication 800-53 (Revision 5) responds to the need by embarking on a proactive and systemic approach to develop and make available to a broad base of public and private sector organizations, a comprehensive set of safeguarding measures for all types of computing platforms, including general purpose computing systems, cyber-physical systems, cloud and mobile systems, industrial/process control systems, and Internet of Things (IoT) devices. Those safeguarding measures include security and privacy controls to protect the critical and essential operations and assets of organizations and the personal privacy of individuals. The ultimate objective is to make the information systems we depend on more penetration resistant to attacks; limit the damage from attacks when they occur; and make the systems resilient and survivable.

American National Standard ISA-62443-4-1-2018: This document is part of a multipart standard that addresses the issue of security for industrial automation and control systems (IACS). It has been developed by working group 04, task group 06 of the ISA99 committee in cooperation with IEC TC65/WG10. This document prescribes the activities required to perform security risk assessments on a new or existing IACS and the design activities required to mitigate the risk to tolerable levels.

Supply Chain:

Framework for Improving Critical Infrastructure Cybersecurity 1.1: The Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes. The Framework consists of three parts: the Framework Core, the Implementation Tiers, and the Framework Profiles. The Framework Core is a set of cybersecurity activities, outcomes, and informative references that are common across sectors and critical infrastructure. Elements of the Core provide detailed guidance for developing individual organizational Profiles. Through use of Profiles, the Framework will help an organization to align and prioritize its cybersecurity activities with its business/mission requirements, risk tolerances, and resources. The Tiers provide a mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk, which will help in prioritizing and achieving cybersecurity objectives.

Nuclear:

NEI 08-09 Cyber Security Plan for Nuclear Power Reactors: The Nuclear Energy Institute (NEI) developed this Standard to assist nuclear energy facilities in meeting cybersecurity regulations required by 10 CFR 73.54 and the NRC. NEI 08-09 describes a defensive strategy that consists of a defensive architecture and set of security controls that is based on NIST SP 800-82 and NIST SP 800-53. Because INGAA is a nongovernment body, a disclaimer will be seen upon selection of this Standard.

NRC Regulatory Guide 5.71: The Nuclear Regulatory Commission, Regulatory Guide 5.71 (NRC RG 5.71), Cyber Security Programs for Nuclear Facilities, provides a framework to aid in the identification of those digital assets, referred to as critical digital assets or CDAs, which must be protected from cyber attacks. The framework offers licensees and applicants the ability to address the specific needs of an existing or new system. Thus the framework provides a flexible programmatic approach in which the licensee or applicant can establish, maintain, and successfully integrate security controls into a site-specific cybersecurity program. The intended audience is owners and operators of nuclear power plants.

Process Control and SCADA:

NIST Special Publication 800-53, Rev. 3 with App I: Appendix I of the NIST SP800-53 adds guidance on industrial control system (ICS) security to the control system guidance already contained in the publication. In this context, an ICS is an information system used to control industrial processes such

as manufacturing, product handling, production, and distribution. ICSs include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCSs), and programmable logic controllers (PLCs). The appendix modifies selected questions and requirements in SP800-53 based on the differences between ICS and typical information systems.

The information in Appendix I is not as comprehensive as that found in NIST SP800-82, but may provide useful information on tailoring, security controls, and control enhancements. NIST guidance was developed for the federal government, but other organizations are encouraged to use it.

NIST Special Publication 800-82: The NIST Guide to Industrial Control Systems (ICS) Security publication provides guidance for establishing a secure ICS including SCADA systems, DCSs, and other systems performing control functions. It identifies typical threats and vulnerabilities to these systems, provides recommended security countermeasures to mitigate the associated risks, and includes a list of many different methods and techniques for securing ICSs.

The scope includes ICSs that are typically used in the electric, water, oil and gas, chemical, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing (automotive, aerospace, and durable goods) industries. This version of SP800-82 is based on the formal publication of the document in June 2011.

NIST Special Publication 800-82, Rev. 1: Revision 1 of the NIST SP 800-82 Standard has the same aims and audience as the earlier version. This revision includes the integration of the ICS material transferred from Special Publication 800-53, Revision 3.

NIST Special Publication 800-82, Rev. 2: Revision 2 of the NIST SP 800-82 Standard has the same aims and audience as the earlier version. This revision includes updates to ICS threats and vulnerabilities, ICS security, ICS risk management, and security capabilities and tools for ICS. It also introduces overlays and provides an ICS overlay for NIST SP 800-53, Revision 4 security controls for tailored security control baselines for Low, Moderate, and High impact ICS.

Supply Chain

NIST SP800-161 Supply Chain Risk Management: Federal agencies are concerned about the risks associated with information and communications technology (ICT) products and services that may contain potentially malicious functionality, are counterfeit, or are vulnerable due to poor manufacturing and development practices within the ICT supply chain. These risks are associated with the federal agencies' decreased visibility into, understanding of, and control over how the technology that they acquire is developed, integrated and deployed, as well as the processes, procedures, and practices used to ensure the integrity, security, resilience, and quality of the products and services. This publication provides guidance to federal agencies on identifying, assessing, and mitigating ICT supply chain risks at all levels of their organizations. The publication integrates ICT supply chain risk management (SCRM) into federal agency risk management activities by applying a multitiered, SCRM-specific approach, including guidance on assessing supply chain risk and applying mitigation activities.

Transportation

Defining a Security Zone Architecture for Rail Transit and Protecting Critical Zones:

This Recommended Practice is Part-II in a series of documents to be released. Part-I released in July 2010 addresses the importance of control and communications security to a transit agency, provides a survey of the various systems that constitute typical transit control and communication systems, identifies the steps that an agency would follow to set up a successful program, and establishes the stages in conducting a risk assessment and managing risk. Part-II presents Defense-In-Depth as a recommended approach for securing rail communications and control systems, defines security zone classifications, and defines a minimum set of security controls for the most critical zones, the, SAFETY CRITICAL SECURITY ZONE (SCSZ) and the FIRE, LIFE-SAFETY SECURITY ZONE (FLSZ). Later parts will cover recommended practices for less critical zones, the rail vehicles, and provide other guidance for a transit agency.

The purpose of this Recommended Practice is to share transit agency best practices; set a minimum requirement for control security within the transit industry; provide a guide of common security requirements to control and operations systems vendors; adopt voluntary industry practices in control security in advance and in coordination with government regulation; and raise awareness of control security concerns and issues in the industry.

TSA Pipeline Security Guidelines, April 2011: This Transportation Security Administration (TSA) document provides a set of short guidelines for protecting and securing the transportation of various liquids through transmission pipelines. It includes cybersecurity guidelines in addition to other security measures including physical protection, personnel security, equipment maintenance and testing, etc. These guidelines are applicable to natural gas and hazardous liquid transmission pipelines, natural gas distribution pipelines, and to liquefied natural gas facility operators. In addition, these guidelines apply to pipeline systems that transport material categorized as toxic inhalation hazards (TIHs).

TSA Pipeline Security Guidelines, March 2018: These guidelines are applicable to operational natural gas and hazardous liquid transmission pipeline systems, natural gas distribution pipeline systems, and liquefied natural gas facility operators. Additionally, they apply to operational pipeline systems that transport materials categorized as toxic inhalation hazards (TIH). TIH materials are gases or liquids that are known or presumed on the basis of tests to be so toxic to humans as to pose a health hazard in the event of a release during transportation.

Questions Only:

Key Questions: The Key Questions are a subset of the Catalog of Recommendations and are limited in scope to what subject matter experts consider to be the top set of requirements. They are geared toward providing meaningful results in a limited amount of time. They should be used only when an assessment based on one or more full Standards cannot be completed within an allotted time. They are intended for any industry using control systems.

Universal Questions: The Universal Questions are based on the Catalog of Recommendations and include a full range of ICS security questions. The questions are written as simple, Yes or No questions and are grouped in a set of common security categories. The Universal Questions are the core set of questions found in CSET and should be included with any questions based assessment.

C2M2 Maturity Indicator Levels

The Cybersecurity Capability Maturity Model (C2M2) Standard uses a system of Maturity Indicator Levels (MILs). They are defined as:

- MIL0: Incomplete
- MIL1: Initiated
- MIL2: Performed
- MIL3: Managed.

They correspond to CSET SALs as follows:

- MIL1: Low
- MIL2: Moderate
- MIL3: High

MIL0 is not used.

Figure 59 shows the MIL to SAL link next to the C2M2 Standard name on the Cybersecurity Standard Selection screen. Clicking this link opens the C2M2 MIL to SAL Conversion window shown in Figure 60 which shows the MIL to SAL mappings.

When selecting the C2M2 Standard, the user should verify that the selected SAL for the assessment corresponds to the desired MIL.



Figure: C2M2 MIL to SAL link

C2M2 MIL to SAL Conversion

The C2M2 standard uses MIL levels instead of SALs. The conversions between those definitions and the CSET SALs are below:

- MIL 1 = Low
- MIL 2 = Moderate
- MIL 3 = High

Close

Figure: C2M2 MIL to SAL Conversion window

CFATS Tiers

The Chemical Facilities Anti-Terrorism Standards (CFATS) Risk-Based Performance Standards Guide 8-Cyber uses Tiers rather than Standard Security Assurance Levels (SALs). To map the CFATS tiers to the SAL options, use the tier designations below.

- Tier I, Very High,
- Tier II, High,
- Tier III, Moderate, and
- Tier IV, Low.

This mapping is reflected on the SAL screen. The CFATS tiers are unrelated to those associated with the Cybersecurity Framework.

Figure 61 shows the Tier to SAL link next to the CFATS Standard name on the Cybersecurity Standard Selection screen. Clicking this link opens the CFATS Tier to SAL Conversion window shown in Figure 62 which shows the Tier to SAL mappings.

When selecting the CFATS Standard, the user should verify that the selected Security Assurance Level (SAL) for the assessment corresponds to the desired Tier.

CFATS Risk-Based Performance Standards Guide 8-Cyber [Tier to SAL](#) Chemical, Oil, and Natural Gas Details ▾

Figure: CFATS Tier to SAL Link

CFATS Tier to SAL Conversion

The CFATS standard uses Tier levels instead of SALs. The conversions between those definitions and the CSET SALs are below:

Tier I = Very High

Tier II = High

Tier III = Moderate

Tier IV = Low

 Close

Figure: CFATS Tier to SAL Conversion window

Cybersecurity Framework Description

This section provides additional information about the Cybersecurity Framework assessment mode. This function was added to CSET in response to Executive Order 13636, Improving Critical Infrastructure Cybersecurity issued on February 12, 2013, which calls for the development of a voluntary risk-based Cybersecurity Framework. The Framework consists of three parts: (1) the Framework Core, (2) the Framework Implementation Tiers, and (3) the Framework Profile.

Framework Core

The Framework Core is a set of cybersecurity activities and references that are common across critical infrastructure sectors organized around particular outcomes. The Core presents Standards and best practices in a manner that allows for communication of cybersecurity risk across the organization from the senior executive level to the implementation/operations level. The Framework Core consists of five functions - Identify, Protect, Detect, Respond, Recover that can provide a high-level, strategic view of an organization's management of cybersecurity risk.

The functions are described as follows:

Identify. Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.

Protect. Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.

Detect. Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

Respond. Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

Recover. Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

The Framework Core then identifies underlying key Categories and Subcategories for each of these functions and matches them with example Informative References such as existing Standards, guidelines, and practices for each Subcategory. This structure ties the high level strategic view, outcomes, and Standards-based actions together for a cross-organization view of cybersecurity activities.

The Framework stems from the principle of common criteria. Common criteria processes are particularly useful as a driving force for the mutual recognition and adoption of secure IT products. By using a common criteria framework, users can develop a common understanding of their security requirements (their protection profile) and communicate these to vendors, business partners, and sector associations.

The Functions and Categories are identified as shown in the figure below.

Function Unique Identifier	Function	Category Unique Identifier	Category Name
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Figure: Function and category identifiers

The Framework Core represents a common set of activities for managing cybersecurity risk. In other words, it presents what owners and operators of cyber assets should do to secure their systems. While it is not exhaustive, it is extensible, allowing organizations, sectors, and other entities to use Subcategories and Informative References that are cost-effective and efficient and that enable the organizations to manage their cybersecurity risk.

As an example, the recommended activities for Asset Management are shown in the figure below. The actions listed under Subcategory will, when implemented, increase cybersecurity and decrease risk. The provided references are the Standards and guidelines from whence the recommended actions were derived.

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	Asset Management (AM): The personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried	<ul style="list-style-type: none"> • ISA 99.02.01 4.2.3.4 • COBIT BAI03.04, BAI09.01, BAI09, BAI09.05 • ISO/IEC 27001 A.7.1.1, A.7.1.2 • NIST SP 800-53 Rev. 4 CM-8 • CCS CSC1
		ID.AM-2: Software platforms and applications within the organization are inventoried	<ul style="list-style-type: none"> • ISA 99.02.01 4.2.3.4 • COBIT BAI03.04, BAI09.01, BAI09, BAI09.05 • ISO/IEC 27001 A.7.1.1, A.7.1.2 • NIST SP 800-53 Rev. 4 CM-8 • CCS CSC 2
		ID.AM-3: The organizational communication and data flow is mapped	<ul style="list-style-type: none"> • ISA 99.02.01 4.2.3.4 • COBIT DSS05.02 • ISO/IEC 27001 A.7.1.1 • NIST SP 800-53 Rev. 4 CA-3, CM-8, CA-9 • CCS CSC 1
		ID.AM-4: External information systems are catalogued	<ul style="list-style-type: none"> • COBIT 5 APO02.02 • ISO/IEC 27001:2013 A.11.2.6 • NIST SP 800-53 Rev. 4 AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	<ul style="list-style-type: none"> • COBIT 5 APO03.03, APO03.04, BAI09.02 • ISA 62443-2-1:2009 4.2.3.6 • ISO/IEC 27001:2013 A.8.2.1 • NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	<ul style="list-style-type: none"> • COBIT 5 APO01.02, DSS06.03 • ISA 62443-2-1:2009 4.3.2.3.3 • ISO/IEC 27001:2013 A.6.1.1 • NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11

Figure: Framework core example

Framework Tiers

Framework Implementation Tiers (Tiers) provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. The Tier selection process considers an organization's current risk management practices, threat environment, legal and regulatory requirements, business/mission objectives, and organizational constraints. The Tiers characterize an organization's practices over a range, from Partial (Tier 1) to Adaptive (Tier 4), progressing from informal, reactive implementations to approaches that are agile and risk-informed.

The figure below lists the risk categories and tier levels. A tier is applied to each of the risk categories. The tiers are described below and presented in relation to each category.

Risk Categories	Tiers
Risk Management Process	Tier 1: Partial
Integrated Risk Management Program	Tier 2: Risk Informed

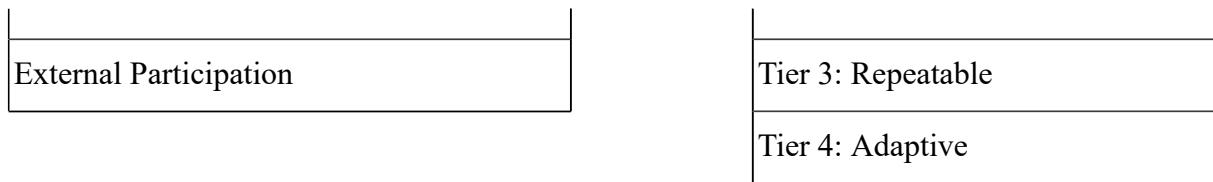


Figure: Risk categories and tiers

Tier 1: Partial

- **Risk Management Process** – Organizational cybersecurity risk management practices are not formalized, and risk is managed in an ad hoc and sometimes reactive manner. Prioritization of cybersecurity activities may not be directly informed by organizational risk objectives, the threat environment, or business/mission requirements.
- **Integrated Risk Management Program** – Awareness of cybersecurity risk is limited at the organizational level, and an organization-wide approach to managing cybersecurity risk has not been established. The organization implements cybersecurity risk management on an irregular, case-by-case basis because of varied experience or information gained from outside sources. The organization may not have processes that enable cybersecurity information to be shared within the organization.
- **External Participation** – An organization may not have the processes in place to participate in coordination or collaboration with other entities.

Tier 2: Risk Informed

- **Risk Management Process** – Risk management practices are approved by management but may not be established as an organization wide policy. Prioritization of cybersecurity activities is directly informed by organizational risk objectives, the threat environment, or business/mission requirements.
- **Integrated Risk Management Program** – There is an awareness of cybersecurity risk at the organizational level, but an organization-wide approach to managing cybersecurity risk has not been established. Risk-informed, management-approved processes and procedures are defined and implemented, and staff has adequate resources to perform their cybersecurity duties. Cybersecurity information is shared within the organization on an informal basis.
- **External Participation** – The organization knows its role in the larger ecosystem, but has not formalized its capabilities to interact and share information externally.

Tier 3: Repeatable

- **Risk Management Process** – The organization's risk management practices are formally approved and expressed as policy. Organizational cybersecurity practices are regularly updated based on the application of risk management processes to changes in business/mission requirements and a changing threat and technology landscape.
- **Integrated Risk Management Program** – There is an organization-wide approach to manage cybersecurity risk. Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed. Consistent methods are in place to respond effectively to changes in risk. Personnel possess the knowledge and skills to perform their appointed roles and responsibilities.

- **External Participation** – The organization understands its dependencies and partners and receives information from these partners that enables collaboration and risk-based management decisions within the organization in response to events.

Tier 4: Adaptive

- **Risk Management Process** – The organization adapts its cybersecurity practices based on lessons learned and predictive indicators derived from previous and current cybersecurity activities. Through a process of continuous improvement incorporating advanced cybersecurity technologies and practices, the organization actively adapts to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner.
- **Integrated Risk Management Program** – An organization-wide approach to managing cybersecurity risk uses risk-informed policies, processes, and procedures to address potential cybersecurity events. Cybersecurity risk management is part of the organizational culture and evolves from an awareness of previous activities, information shared by other sources, and continuous awareness of activities on their systems and networks.
- **External Participation** – The organization manages risk and actively shares information with partners to ensure that accurate, current information is being distributed and consumed to improve cybersecurity before a cybersecurity event occurs.

Successful implementation of the Framework is based on achievement of the outcomes described in the organization's Target Profiles and not on Tier determination.

Framework Profiles

The Framework Profile (Profile) is the alignment of the Functions, Categories, and Subcategories with the business requirements, risk tolerance, and resources of the organization. A profile enables organizations to establish a roadmap for reducing cybersecurity risk that is well aligned with organizational and sector goals, considers legal/regulatory requirements and industry best practices, and reflects risk management priorities. Given the complexity of many organizations, they may choose to have multiple profiles, aligned with particular components and recognizing their individual needs.

Framework Profiles can be used to describe the current state or the desired target state of specific cybersecurity activities. They support business/mission requirements and aid in the communication of risk within and between organizations. They can reveal gaps to be addressed to meet cybersecurity risk management objectives. Profiles can be used to conduct self-assessments and communicate requirements and results within an organization or between organizations.

Framework Implementation Tiers

If Cybersecurity Framework is selected as the assessment mode, the screen will allow for assignment of the framework tiers. Framework tiers are not related to the CFATS tiers. The figure below shows the screen when Cybersecurity Framework-based and the Implementation Tiers tab are selected.

The screenshot shows the CSET interface with the 'Cybersecurity Framework' selected as the assessment mode. The top navigation bar includes links for 'Tools', 'Resource Library', 'Help', and 'Your Username'. Below the navigation is a toolbar with tabs for 'Prepare', 'Diagram', 'Questions', and 'Results'. The main content area is titled 'Cybersecurity Framework' and contains a section titled 'External Participation' with four levels: Tier 1, Tier 2, Tier 3, and Tier 4. Each tier has a description. Below this is a section titled 'Integrated Risk Management Program'.

Cybersecurity Framework

Select the cybersecurity framework profile you want to use for your assessment. The baseline cybersecurity framework profile comes preloaded with CSET that you can copy to get started when creating your own custom profiles. You can also create a new custom profile or update and export existing profiles.

External Participation

- Tier 1**
An organization may not have the processes in place to participate in coordination or collaboration with other entities.
- Tier 2**
The organization knows its role in the larger ecosystem, but has not formalized its capabilities to interact and share information externally.
- Tier 3**
The organization understands its dependencies and partners and receives information from these partners that enables collaboration and risk-based management decisions within the organization in response to events.
- Tier 4**
The organization manages risk and actively shares information with partners to ensure that accurate, current information is being distributed and consumed to improve cybersecurity before a cybersecurity event occurs.

Integrated Risk Management Program

Figure: Cybersecurity Framework screen

Implementation Tiers: The Implementation Tier list indicates the framework tier level for the selected risk category. Users should select the tier that most accurately describes their organization.

Mode Selection

Mode Selection is available at the top of the Questions/Requirements page and allows the user to determine the general approach they want to take with completing the assessment. The figure below describes the Mode Selection screen.

The screenshot shows the CSET interface with the 'Questions' tab selected. At the top, there are tabs for 'Prepare', 'Diagram', 'Questions' (which is highlighted in blue), and 'Results'. Below the tabs, there are two buttons: 'Questions Mode' (selected) and 'Requirements Mode'. On the right side, there are buttons for 'Collapse All' and 'Expand All', and a checkbox for 'Auto-load Supplemental'. The main content area is titled 'Access Control - Standard Questions' and contains a section titled 'Access Agreements'. It asks if there are any access agreements for third party access. The response is marked as 'Yes' (green). Below this, there are two numbered questions: 1. Are appropriate agreements finalized before access is granted, including for third parties and contractors? and 2. Are access agreements periodically reviewed and updated? Both questions have green 'Yes' buttons and grey 'No', 'NA', and 'Alt' buttons. There are also small icons for each question.

Figure: Mode Selection screen

Questions Mode: The Questions-based approach will ask simple questions during the assessment. The questions are determined from requirements based on the selected cybersecurity standard. All questions are scored in the final results. Most advanced users will select the Questions-based approach.

Requirements Mode: The Requirements-based approach uses the exact wording of requirements from the selected Standard as questions and each requirement must be fully met in order to meet the requirement. This approach is best used by industries that are regulated by a specific standard.

Assessment Mode

This section provides additional information on the three available advanced assessment modes on the Assessment Mode Selection screen of the CSET tool.

Questions-based Approach:

A comprehensive set of questions has been prepared with straightforward language that encompasses all the topics and requirements found in the major industrial control system (ICS) and information technology (IT) Standards. Each question is written in such a way that it can be answered as either Yes or No. (Questions can also be answered by using alternates or not applicable; however, they do not use multi-part answers.) The full set of questions is filtered and limited by the Standards selected and by the SAL. The Questions mode is recommended for most assessments and is set by default.

Requirements-Based Approach:

The Requirements mode was developed primarily for regulated industries such as nuclear or electrical power. This mode is designed so that the user will see the exact wording of each requirement in the Standard. The question must be read and answered in its entirety.

Questions-based Approach

If the Questions-based Approach is selected then most of the Standards will be available. Select the Standard or Standards that apply to the system and industry or sector being evaluated.

If only one Standard is selected, the Key Questions offer a small selection of the top set of requirements designed for assessments of limited scope or time while the Universal Questions offer the most comprehensive, general evaluation.

If multiple Standards are selected, the questions will be the superset of all selected Standards. It is recommended that the Universal Questions be included. The Standards may have some questions that are so unique that they are not included in the universal set. This means that selecting both the Universal Questions and a Standard will result in a set of questions that is potentially greater than the Universal Questions themselves. These situations are described in detail below.

In the figure below, three cases are presented. (In 1 and 2, there is no consideration for the SAL.)



Figure: Question sets for questions mode

Case 1. In this scenario, only the Universal Questions option has been selected. As shown in the diagram, all the Universal Questions are displayed.

Case 2. This scenario shows two options. If only Standard A was selected, then only those questions included in the inner circle would be presented. The Universal Questions outside the inner circle would not be included in the assessment. The second option shows where both Standard A and the Universal Questions were selected.

Because the Standard is completely included in the Universal Question set, the resulting assessment questions would look exactly like Case 1, the Universal Question set.

Case 3. Unlike the example in Case 2, the selected Standard B has extra questions not found in the Universal Question set. If only Standard B was selected then everything shown in the ellipse would be displayed in the assessment. If both the Standard and Universal Questions sets were selected, then the total assessment would be greater than what is included in Case 1 and would include the combination of both the round (Universal) and ellipse (Standard B) shapes.

Requirements-based Approach

If the Requirements-based Approach is chosen, then the Universal Questions option is disabled. If multiple Standards are selected, then for each choice a completely different set of requirements will be displayed. In the figure below, two cases are presented.

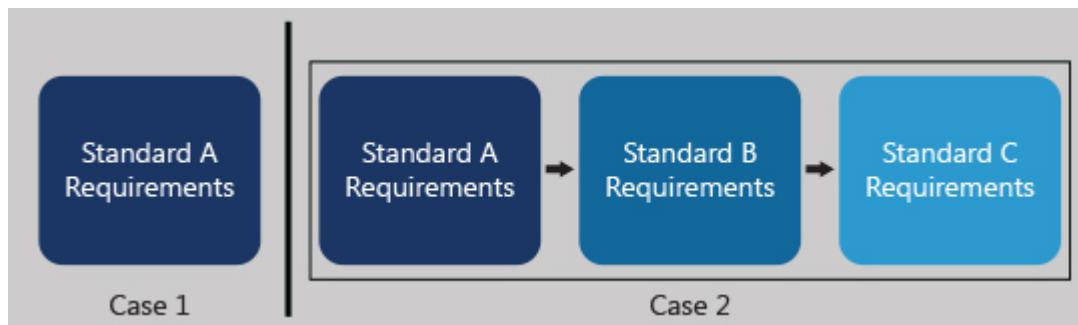


Figure: Requirements mode

Case 1. In this scenario, a single Standard has been selected, and only the requirements for Standard A will be presented in the Questions screen.

Case 2. This second scenario shows the selection of multiple Standards. No matter how many Standards are selected, the tool will display the full set of requirements for each set regardless of any overlap. Because the wording in the Standard is unique, each requirement will be given verbatim. In the application, the requirements in the Standards will simply show up on the question tree in a sequential manner.

Standards Available in Both Modes

Many Standards are available in both the Questions mode and the Requirements mode. In Questions mode, statements from the Standard may be split apart to form several questions so that the user may get partial credit for complying with a portion of the requirement. It also makes each question shorter, more direct, and easier to understand. In Requirements mode, the requirement statement is presented as written in the Standard. It may be longer and encompass several compliance activities. Partial compliance is considered a Fail in this mode.

Diagram Screen

Building a Network Diagram

This section provides detailed instructions for creating a network diagram and using the diagramming tool. The diagram may be created within CSET or imported from ones created in previous releases of CSET.

CSET includes a drawing tool that is valuable in several ways.

- First, it provides a place to graphically capture a picture of the control system or information technology (IT) network.
- Second, it incorporates simple network analysis features to identify areas of vulnerability and recommendations for protection.
- Third, it is used to create the foundation for the question set that is incorporated into the overall assessment and analysis.

With this drawing tool, the user is able to:

- Build the diagram from scratch using the drawing tools and available objects and shapes.
- Import a pre-built template from a list of templates provided with the tool.

Diagram Section

After starting an assessment and completing the Prepare section the user will see the screen in the figure below. Click the "Create a network diagram" to begin. If the user has already started a diagram the button will read "Edit the network diagram". Clicking Diagram Inventory opens a separate page. To learn more about the [Diagram Inventory](#), see the help section.

The screenshot shows the CSET software interface with a dark blue header bar. The header contains the CSET logo, a lock icon, 'Tools' with a dropdown arrow, 'Resource Library', a help icon with 'Help' and a dropdown arrow, and a user icon with 'Your Username' and a dropdown arrow. Below the header is a navigation bar with tabs: 'Prepare' (selected), 'Diagram' (highlighted in blue), 'Questions', and 'Results'. The main content area has a white background and a title 'Diagram and Network Component Selection'. Below the title is a paragraph: 'Building a diagram of your system's network allows CSET to include component specific questions in your final questions set. This step is not required but completing a network diagram has several benefits:'. A bulleted list follows: • Graphically capture a picture of your control system or information technology (IT) network. • Identify areas of vulnerability in your network and review recommendations for improvement. • Creates a foundation for the question set incorporated into the overall assessment and analysis process. At the bottom of the content area are two buttons: 'Edit the network diagram' and 'Diagram Inventory'. On the left side of the bottom bar is a 'Back' button, and on the right is a 'Next' button. A small upward arrow is located at the bottom center of the page.

Figure: Diagram section

Diagram Screen Layout

After starting an assessment and completing the Prepare section you will see the diagram screen with the Template dialogue open.

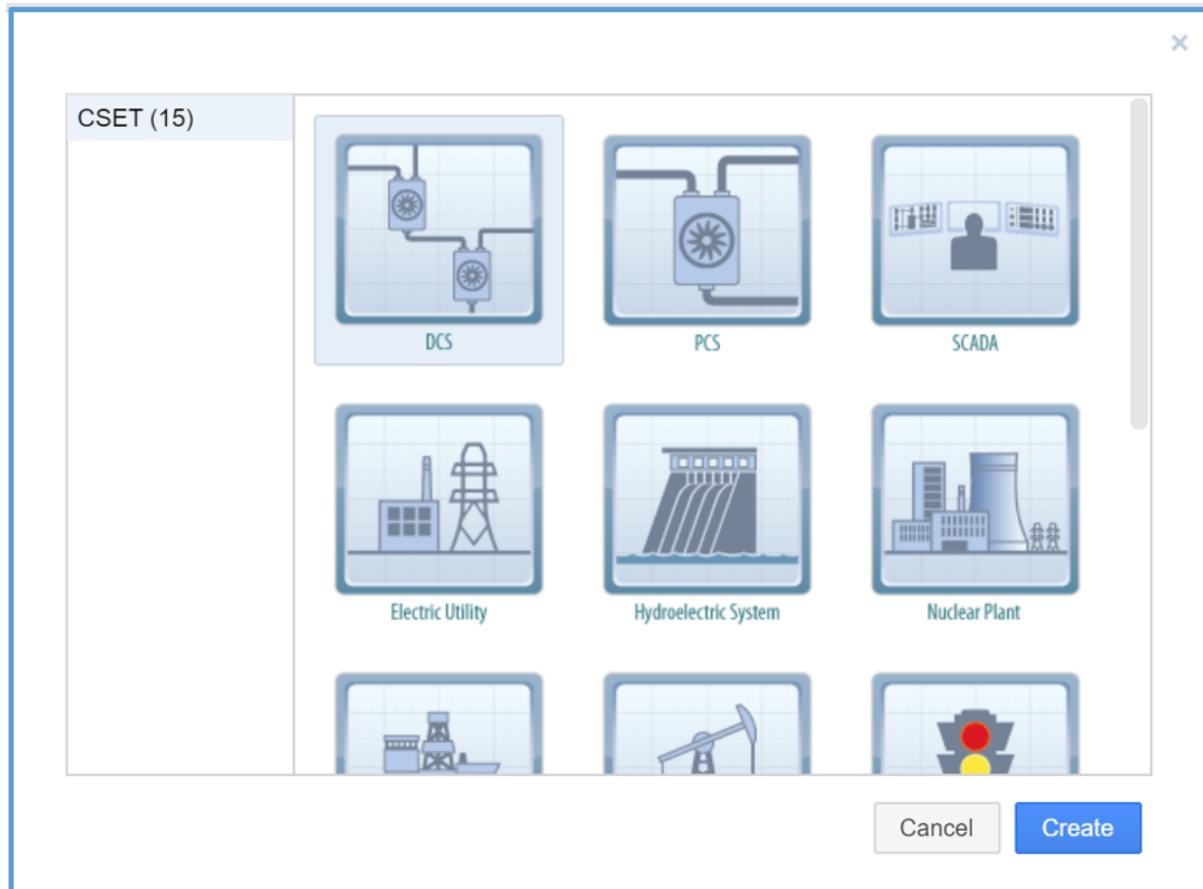


Figure: CSET Template dialogue

You can select a predefined CSET template and then select Create to open it on the diagram screen. If you want to start with just a blank diagram screen select Cancel. For more information on Templates, see the [Home- File Menu](#) -> New from Template section.

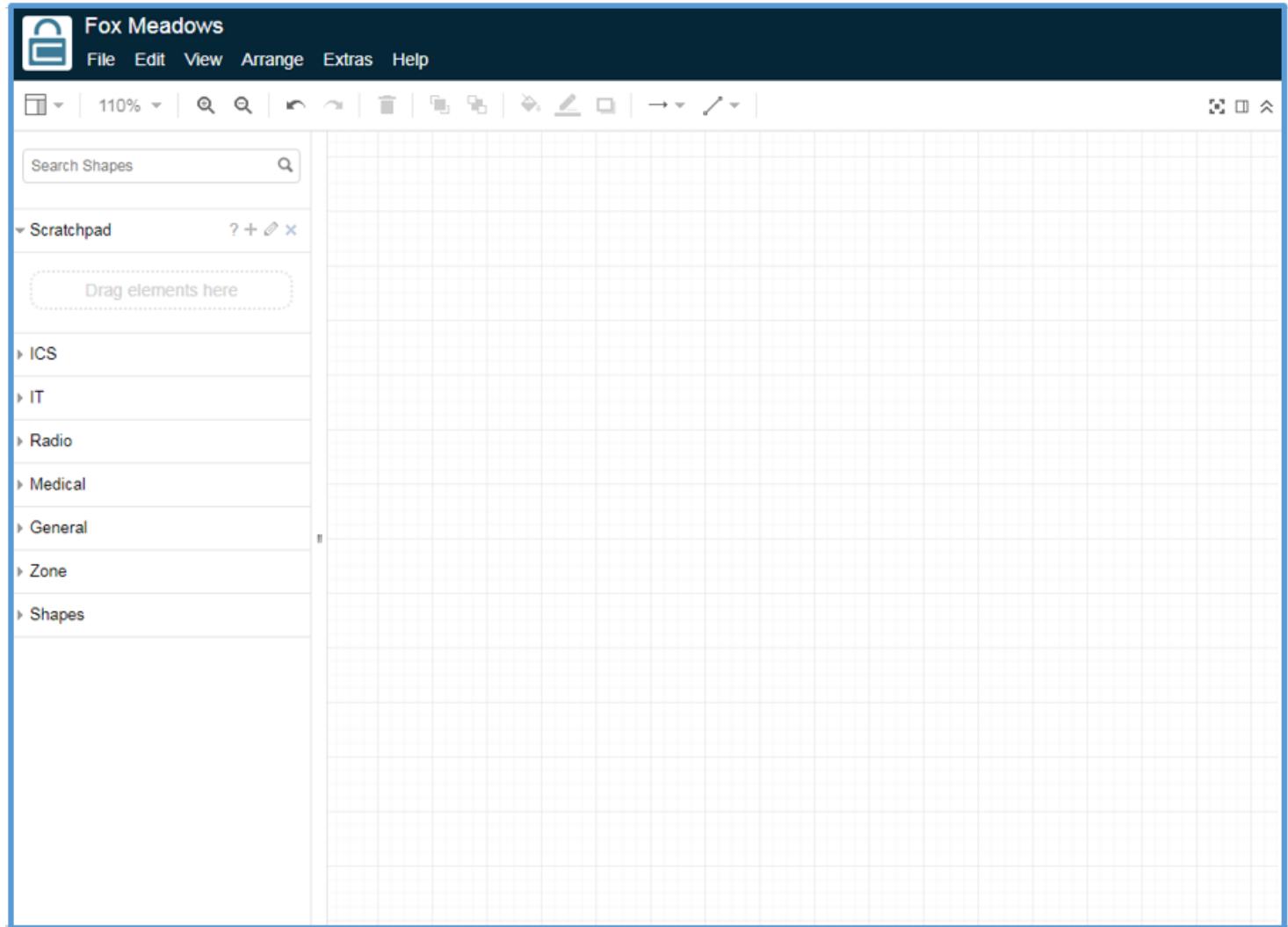


Figure: Diagram screen with no template selected

To maximize the drawing area, use the show/hide arrows in the tool bar (shown in yellow). Clicking this will cause the home menu to collapse.

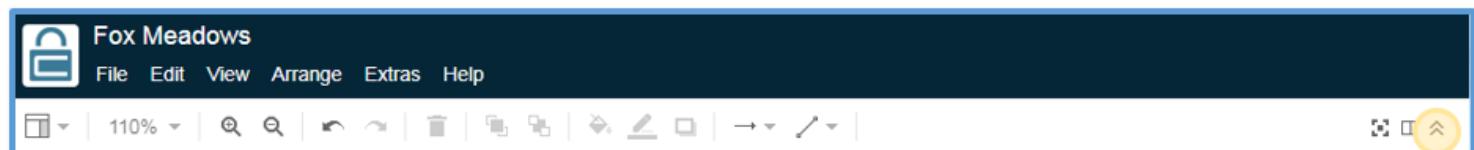


Figure: Maximized drawing area

Screen Parts

Symbols panel

The Symbols panel is on the left and contains a mix of stencils with shapes, zones, components, and text. It contains icons for all the CSET control system and network components plus zones and general shapes that are to be used in the tool. The icons within the panels can be dragged and dropped onto the drawing area to create or modify a network diagram. These icons are specifically designed for CSET and cannot be copied and pasted into other applications.

Shown below in blue in the image below.

Diagram menu bar

The Diagram menu bar consists of six menus: File, Edit, View, Arrange, Extras, and Help.

Shown below in orange in the image below.

Diagram tool bar

The ribbon is at the top of the drawing area and has options for altering the drawing area, sizing, undo/redo, delete icons, bring to front/send to back, color, shadow, and connectors.

Shown below in yellow in the image below.

Drawing Area

This is the main part of the window and is where the icons are placed to create or modify the network diagram.

Shown below in green in the image below.

Format panel

The Format panel is on the right side and allows the user to edit the diagram objects.

Shown below in purple in the image below.

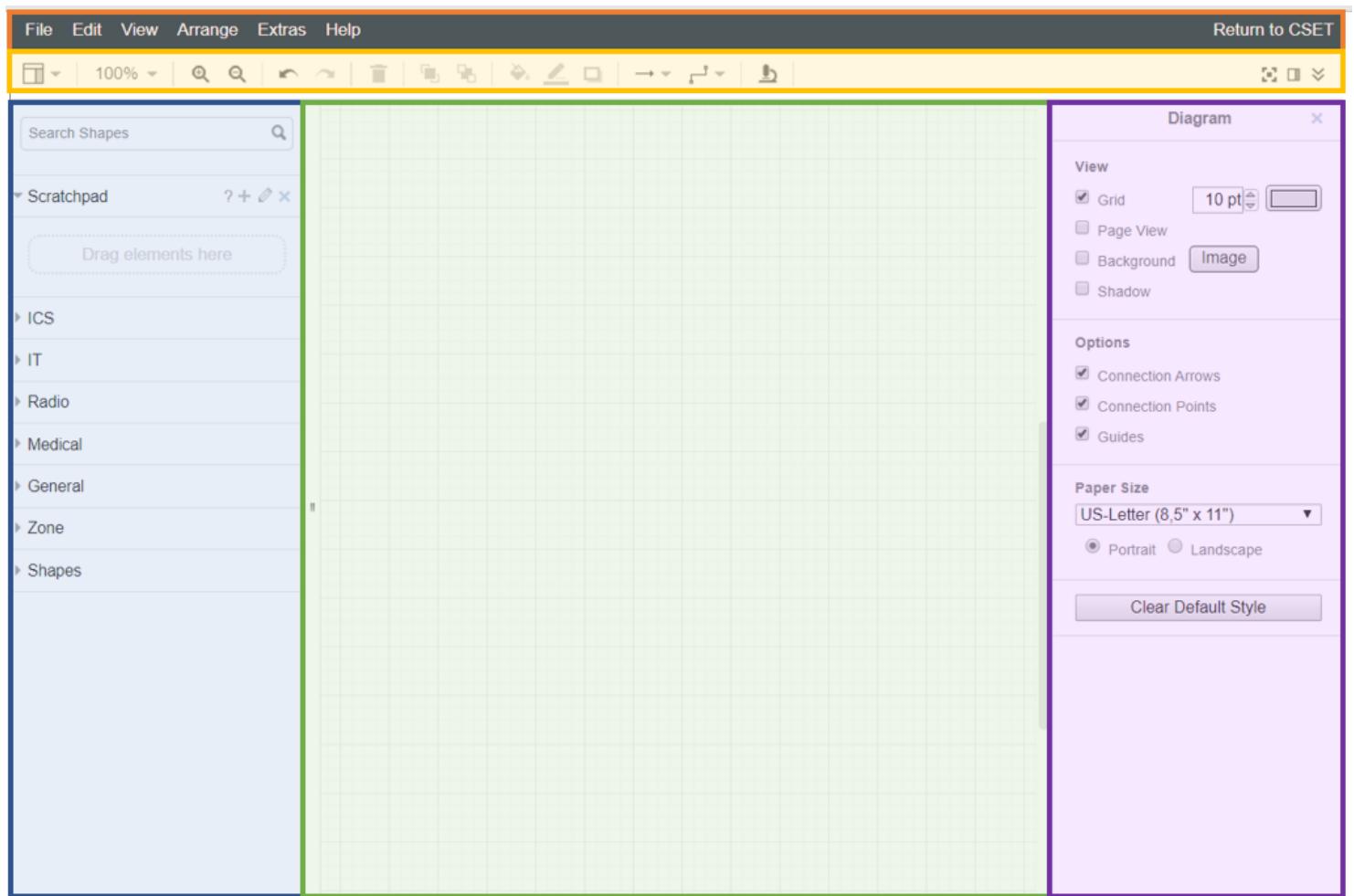


Figure: Diagram screen parts

Diagram Inventory

Clicking "Diagram Inventory" from the Diagram page opens the page below. The Diagram Inventory lists all the items contained in the network diagram including components, zones, shapes, and links. Click the tabs at the top to see the items of interest.

Note: The Diagram Inventory is available from the [Diagram Section](#) screen. If you are in the Diagram tool you will not have access to the inventory.

The screenshot shows the 'Diagram Inventory' screen with the following interface elements:

- Top navigation bar with tabs: Prepare, Diagram (selected), Questions, Results.
- Title: Diagram Inventory.
- Buttons: Export to Excel, Return to Diagram.
- Table header: Components, Zones, Shapes, Text, Links, Network Warnings.
- Table columns: Label, Has Unique Questions, Sal, Criticality, Layer, IP Address, Asset Type, Zone, Subnet Name(s), Description, Host Name, Visible.
- Data rows:
 - External Firewall: Main Layer, Firewall, Corporate-Low, checked
 - Public Historian: Main Layer, Historian, Corporate-Low, checked
 - Corp IDS: Main Layer, Intrusion Detection System, Corporate-Low, checked
 - Connector_4a: Main Layer, Connector, Corporate-Low, checked
 - Corp Router: Main Layer, Router, Corporate-Low, checked

Components		Zones		Shapes		Text		Links		Network Warnings	
Label	Has Unique Questions	Sal	Criticality	Layer	IP Address	Asset Type	Zone	Subnet Name(s)	Description	Host Name	Visible
External Firewall	<input type="checkbox"/>			Main Layer		Firewall	Corporate-Low				<input checked="" type="checkbox"/>
Public Historian	<input type="checkbox"/>			Main Layer		Historian	Corporate-Low				<input checked="" type="checkbox"/>
Corp IDS	<input type="checkbox"/>			Main Layer		Intrusion Detection System	Corporate-Low				<input checked="" type="checkbox"/>
Connector_4a	<input type="checkbox"/>			Main Layer		Connector	Corporate-Low				<input checked="" type="checkbox"/>
Corp Router	<input type="checkbox"/>			Main Layer		Router	Corporate-Low				<input checked="" type="checkbox"/>

Figure: Diagram Inventory screen

If desired, the list may be exported to Excel as a spreadsheet as seen in the image below. The list is included in the Security Plan report as well.

Diagram Component Inventory20.xls [Compatibility Mode] - Microsoft Excel

The screenshot shows a Microsoft Excel spreadsheet titled "Diagram Component Inventory20.xls [Compatibility Mode] - Microsoft Excel". The ribbon menu is visible at the top, showing tabs for File, Home, Insert, Page Layout, Formulas, Data, Review, View, and Team. The Home tab is selected. The ribbon also includes icons for Paste, Clipboard, Font, Alignment, Number, Styles, Cells, Editing, and MindManager.

The main content area displays a table with the following data:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	Tag	HasUniqueQuestion	SAL	Criticality	Layer	IPAddress	AssetType	Zone	Subnets	Description	HostName	IsVisible		
2	HMI-1	False	Moderate	Moderate	Bldg 101		HMI					FALSE		
3	AS-2	False	Low	Moderate	Main Lan		Application	Zone-1				TRUE		
4	EW-3	False	Low	Moderate	Main Lan		EWS	Zone-1				TRUE		
5	DB-4	False	Moderate	Moderate	Main Lan		DB Server	Zone-2				TRUE		
6	HMI-5	False	Moderate	Moderate	Main Lan		HMI	Zone-2				TRUE		
7														
8														
9														
10														
11														
12														
13														
14														
15														
16														
17														
18														
19														
20														
21														
22														
23														
24														
25														
26														
27														
28														
29														
30														

The status bar at the bottom shows tabs for Network Components, Multiple Services Components, Network Zones, and Network, with Network currently selected. It also shows a zoom level of 100%.

Figure: Excel output from the diagram inventory

Clicking the "Return to Diagram" button on the top right of the screen takes the user back to the Diagram screen.

Drawing the Network Diagram

There are a couple different ways to start drawing a network diagram. The first approach is to use a template. The templates included in the diagram tool are generic for a particular sector or control system type.

When you first begin a new diagram a popup for selecting a template will open. If you want to begin with a template, select from the list. The included template types are: DCS, PCS, SCADA, Electric Utility, Hydroelectric System, Nuclear Plant, Oil & Gas System 1, Oil & Gas System 2, Traffic Control, Waste Water Treatment Plant, Water Plant System, HVAC, Building Access Control, Medical, and Radio.

To select a template after starting a diagram, go to the File menu tab and select New from Template. Clicking the button will open the same list of templates that opens upon starting a new diagram. When you select a template from the available list, the system will load the components, network connectors, and zones in the diagram. You will need to modify the components and the layout to match your system.

The second approach is to start a diagram from scratch. You do so as follows:

- 1) Click and drag an ICS component icon from the Symbols panel onto the drawing area. Continue to drag components onto the diagram until you have placed those that you need.
- 2) Add metadata for each icon, such as the label, IP address, criticality, Host Name, and Description. The SAL is inherited from the Zone or overall assessment. Metadata options change based on the shape selected.
- 3) Connect the components using line connectors. See the Help section titled [Adding Links](#) for more details.
- 4) Add zones with the necessary diagram properties, and then move the respective components into the zone boundaries. See the Help section titled [Adding Zones](#) for more information.
- 5) Add any labels, shapes, or text to polish the diagram. See the Help sections labeled [Adding Text](#) and [Adding Shapes](#) for more information.
- 6) Continue to add to, remove, or edit the icons until the diagram is complete.
- 7) Use the Save As to download the diagram as a physical file. Use the Export As to export the diagram as a .PNG, .JPEG, .SVG, .VSDX, or use the Advanced Feature to specify the file type, size, background, and border of the file being exported.

Adding Components

To add a new component icon to the diagram, you will need to select it from the left side Symbols panel. For the following example, adding a component will be discussed. See the image below. The process is similar for adding a shape or zone.

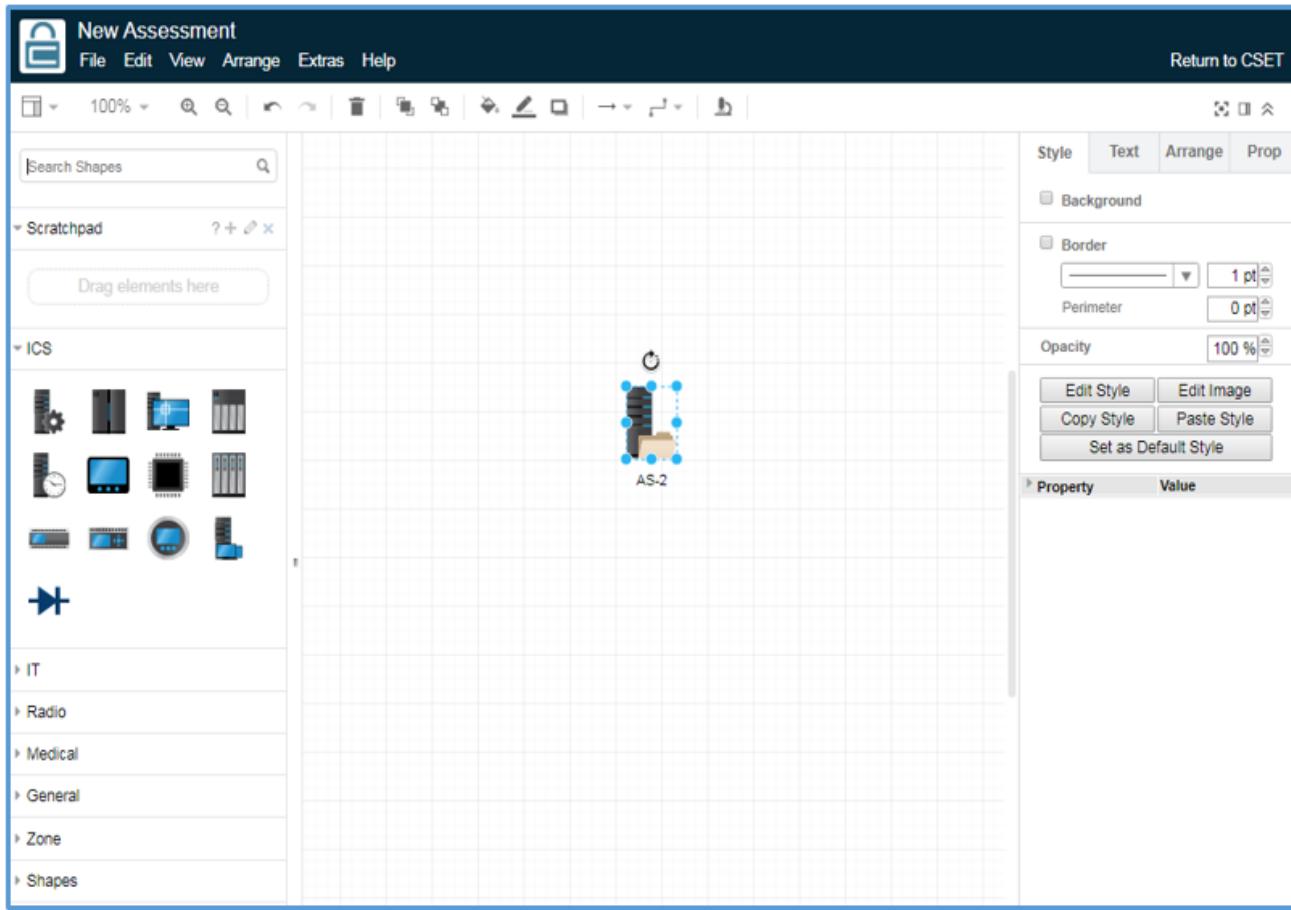


Figure: Placing a component

In this example, the user has clicked on the Application Server icon from the Components list and while holding the mouse down, dragged a copy of the icon onto the drawing area. The selected icon is highlighted. While the frame is displayed you can select a corner to change the size of the icon. You can also rotate the icon using the handle shown above. If you click within the box, you can drag the component across the screen. You can also move the selected component by using the keyboard arrows.

Some devices may be physically contained within a single shell such as a firewall and intrusion detection system (IDS). In such a case, a logical combination of the firewall and the IDS icons should be placed on the diagram. Or, the Multiple Services Component may be used to group the device icons.

Clicking the icon will open the Format panel with diagram properties and formatting options for the symbols on the right side of the screen.

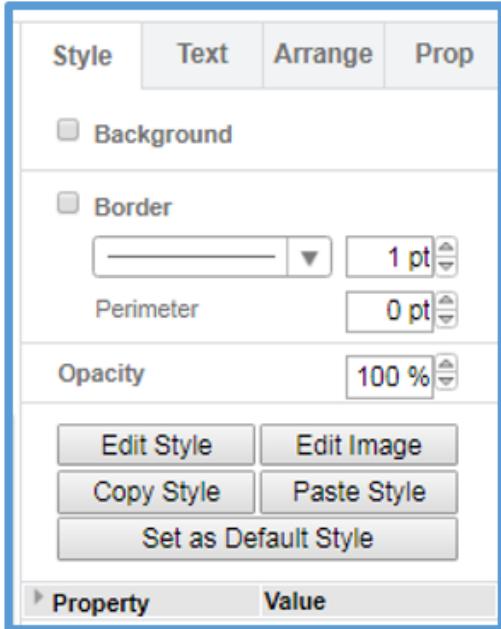


Figure: Symbol with properties panel open

Component Options

Style tab

The options under the Style tab include background, border, opacity, edit/copy/paste/set as default, and view the property details.

Text tab

Under the text tab, the attribute of any embedded text can be changed such as the font, the size, position, spacing, and the text color.

Arrange tab

The arrange tab provides the ability to resize, position, rotate, flip, and angle the symbols.

Property tab

Options under the property tab include designations of label, the SAL, IP address, asset type, criticality, unique questions checkbox, a description field and a host name.

Symbol Properties

Label: This is the common name used to refer to the component. This name will be used in the Questions screen, the analysis, and the reports. It should be the name that people are most familiar with. While not required, ideally these names should be unique. Examples may be Main Historian, Corp Firewall, Pump House HMI, etc.

SAL: This field is only applicable to a zone object and allows you to change the [security assurance level](#) (SAL) for that specific zone. This can be helpful in separating areas of the facility into those areas that need greater protection and those that do not.

If, for example, you have an overall SAL of High based on the consequences of an event happening at the facility and you do not use zones and do not change the SAL level, then all component questions that are marked as High will be presented. If you changed a particular zone to Low, because it was not included in the critical areas, the question set would be smaller and would be less rigorous than the High questions. The zone approach allows you to minimize costs and use of limited resources, while still providing the appropriate levels of protection for your site.

IP Address: This field is only for your reference. It is not used by CSET at this time and is for you to capture the Internet Protocol address information if you wish.

Asset: This field displays the asset or component type. It is used to help identify the selected component. The type may be modified by using the drop-down selection box. Changing the type will automatically change the icon on the drawing. The Tag will also change to indicate the new type unless it was modified by the user or if the diagram was created in an earlier version of CSET.

Criticality: This field allows you to adjust the relative importance of a particular component as compared with others on the diagram. When you place a component on the diagram, the default setting will be moderate. If the component is of lesser importance, then it can be changed to Low. Conversely, if the component is of greater importance to the system, then it should be changed to High.

The level captures the relative importance of unique components in the diagram and can be used in planning, design, and maintenance decisions.

Host: This is the official network name for the piece of hardware. Often the organization will keep a database or inventory of assets, including network equipment. The name in the inventory may have a property number that is unique but may not be remembered by most people. An example might be ACME1-43222-AC-22. The Host Name is useful for verification of exact equipment, but is not used elsewhere in CSET at this time.

Has Unique Questions: This is an important option for identifying a component that is different from other components of that type in the system. By marking a component as being unique, you are instructing the tool to create a separate full set of questions for the device. This means that the default questions that are answered for all components in the system, or even for those of a given type, will not propagate to any component marked as unique.

As an example, you may have five servers in your facility, and four of those have been replaced in the last year with new models. These four are configured with the latest policies and take advantage of features inherent in a new operating system and other improved utilities. The fifth server is several years old and uses technology from an earlier period. In this situation, the fifth server should be marked as unique, so that the answers related to the four new servers are not assigned to the older fifth server.

There are a few components, like the web, that have no questions assigned to them. The Has Unique Questions box will be dim or disabled when no question sets are associated with a particular component.

Description: This optional field allows the user to add descriptive text about the component.

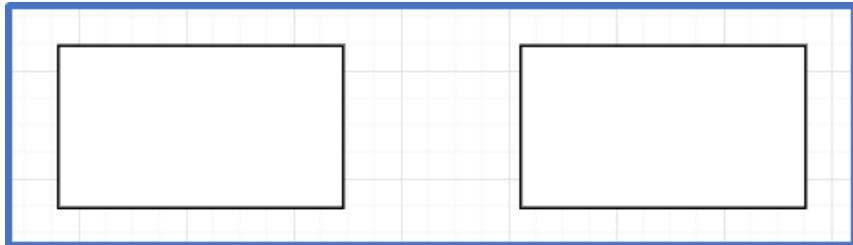
If you click on a zone the property tab will show a "type". It's a dropdown which you can use to change the [zone type](#).

Adding Links

There are two ways to attach a connector to a shape. There are anchored connections, or a floating connections. Links may be referred to as links, lines, or connectors.

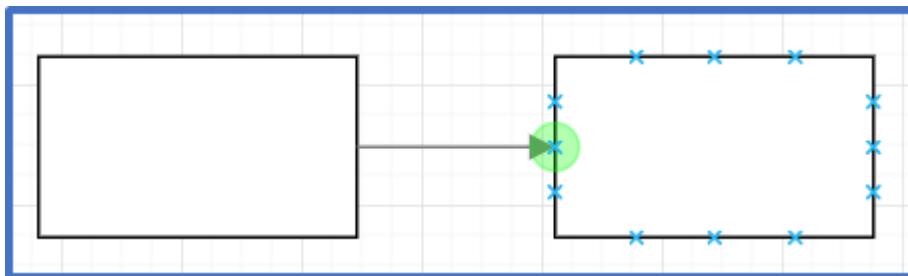
Anchored Connectors

For this example, connect two rectangles.

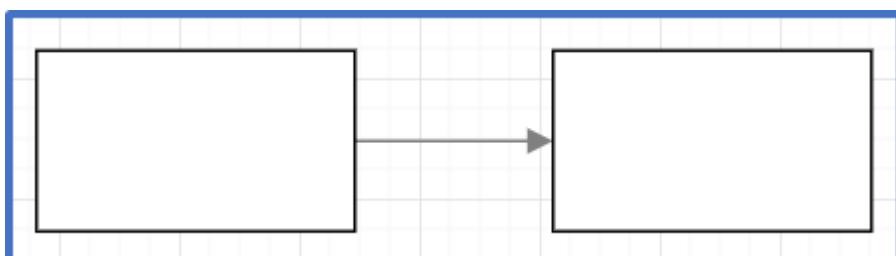


You can connect two shapes by finding a connection point on the first shape, and then click and drag until a connection point is found on the second shape.

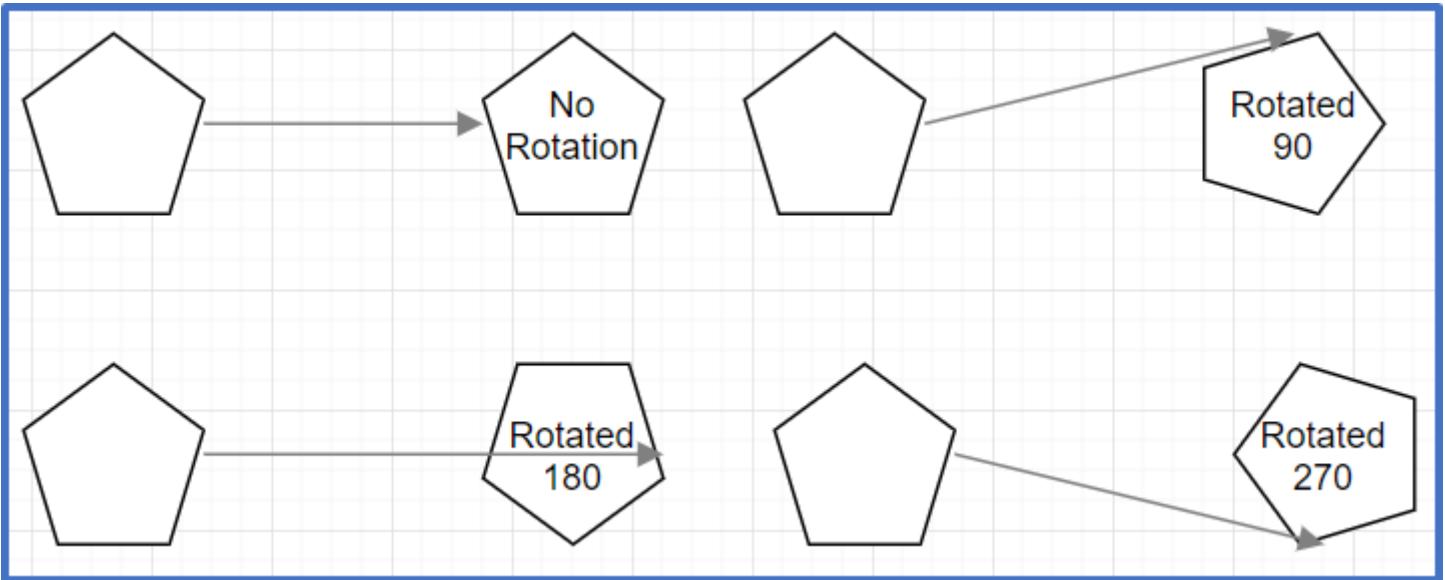
Fixed connection points (anchored connectors) are indicated with small blue crosses. Once you have found a connection point, with the cursor, it will highlight in green.



Release the connection here. Now there is an anchored connection point. This means that as the shape moves, the connector will always remain attached to the same connection points. In the example, both ends of the connector are anchored.



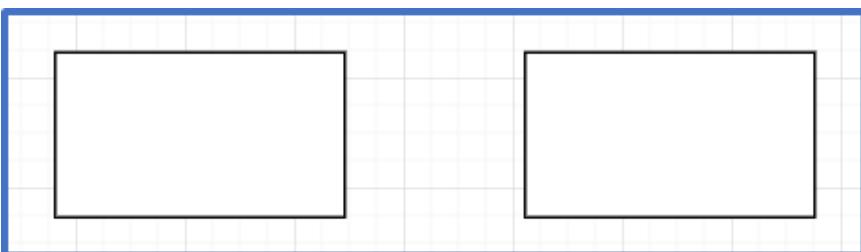
One of the best ways to illustrate how this works is to rotate one of the shapes multiple times.



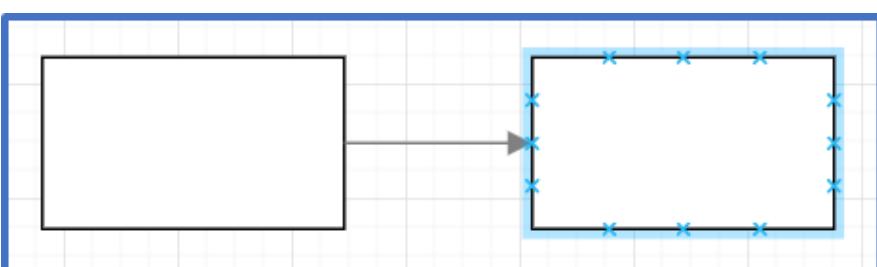
You can see that the connector follows the connection point. There would be the same thing if the first shape was rotated.

Floating Connectors

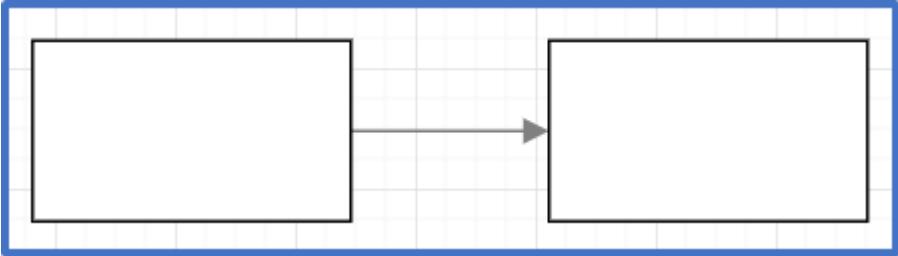
There is another way to connect those two rectangles.



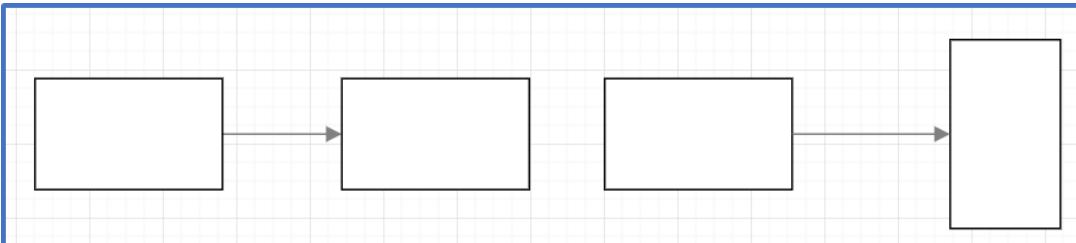
Find a connection point on the first shape, then click and drag as before. But this time, drag the connector over the center of the second shape, so that the whole shape is outlined in a solid blue line.



Release the connection here. Now there is a floating connection point. This means that as the shape moves, the connector adjusts the connection point that it connects to. Notice that it looks identical to an anchored connection point.



However, if the second shape is rotated there is a difference.



There are several ways to create a connection between two points. This section has been about creating a connection to an existing shape. There are also ways in which you can create a new shape, while creating a connection to it at the same time. One way is to use the arrow symbol on the right-hand side of a highlighted shape.

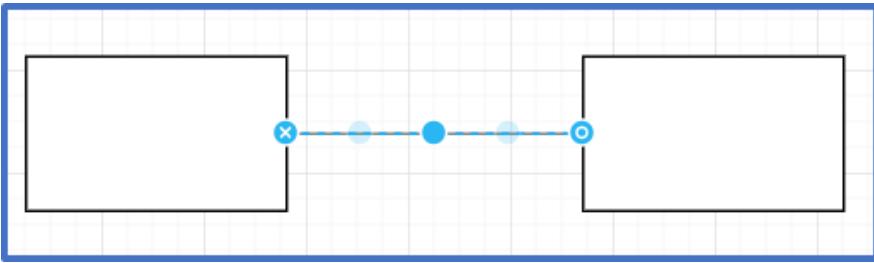
	Start Connection	End Connection
CONNECT TO EXISTING SHAPE		
Drag to edge connection point	Anchored	Anchored
Drag to centre	Anchored	Floating
CREATE NEW SHAPE AND CONNECT		
Clicking arrow symbol to copy	Floating	Floating

Figure: Connections definition table

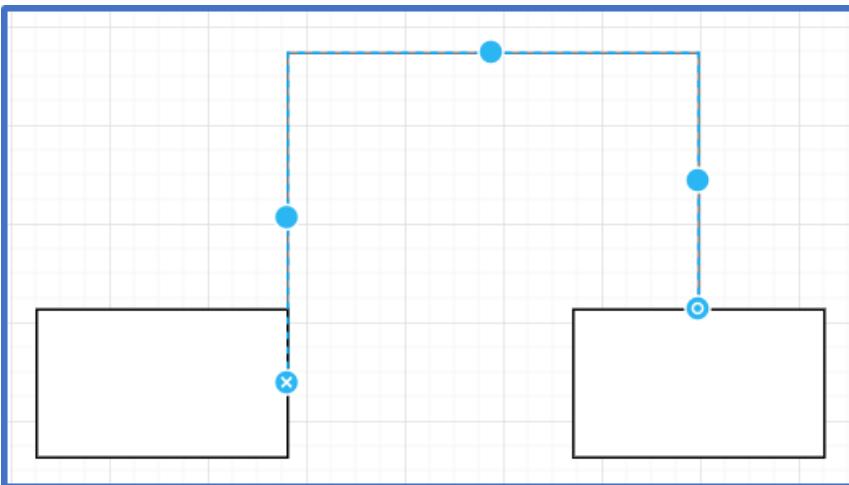
Waypoints

It is possible to arrange connections in different ways. This is often useful in more complex diagrams, where connectors between different shapes might need to avoid any intervening shapes. Also, the orthogonal connectors that have been used so far might not be the most appropriate choice. You can incorporate various types of connector shapes with waypoints.

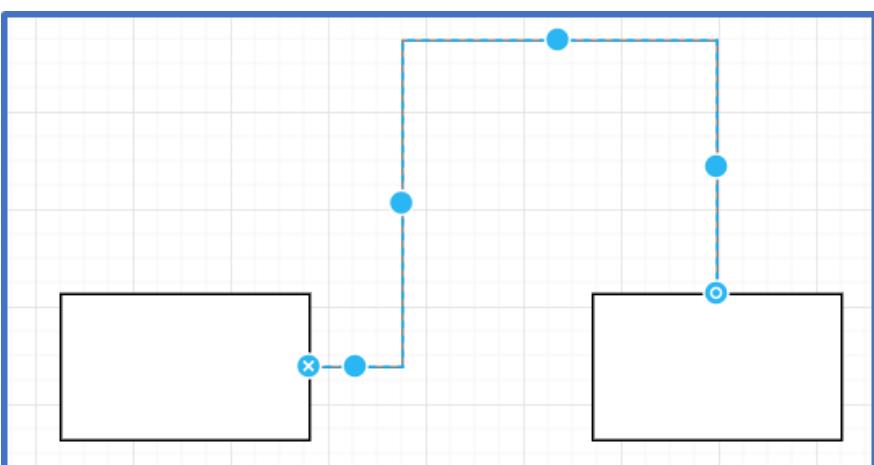
Start with a simple diagram: two rectangles, linked by a connector. The start of the connector is anchored to the first rectangle. The end of the connector has a floating connection to the second rectangle. Click on the connector to highlight it.



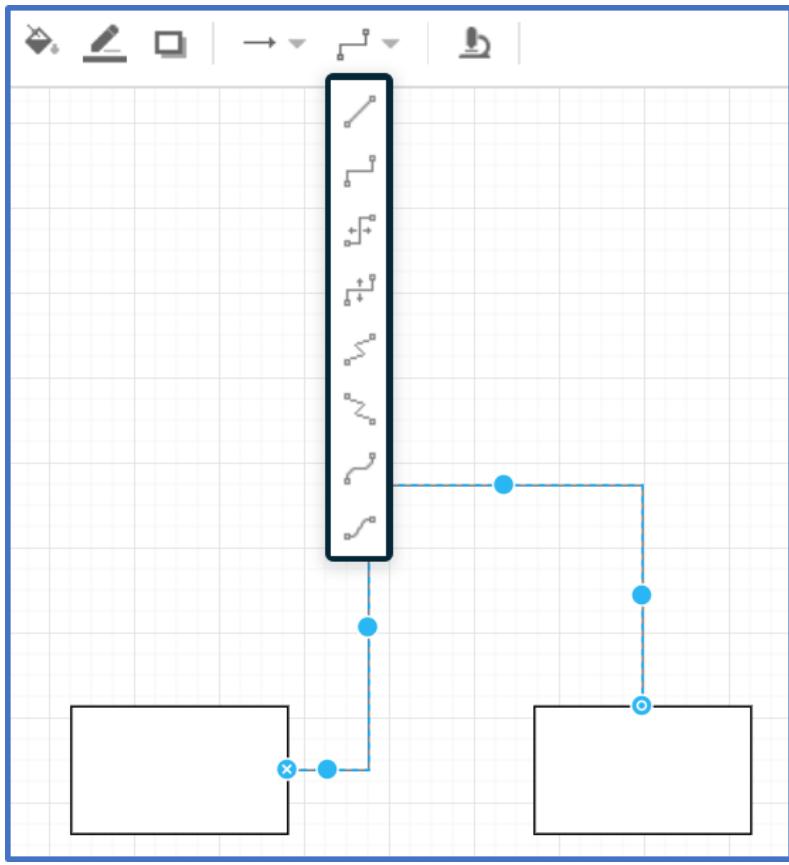
You can see that there is a blue dot in the middle of the connector. This is a waypoint. It's used to change the path of the connector. Click and drag the blue dot upwards.



That changes the path of the connector. Note that the ends of the connector - one anchored, the other floating - both behave as expected. As new sections of the connector are created, more waypoints appear, to allow further manipulate the path. Choose one of the new waypoints, the one above the first rectangle, and drag it slightly to the right.

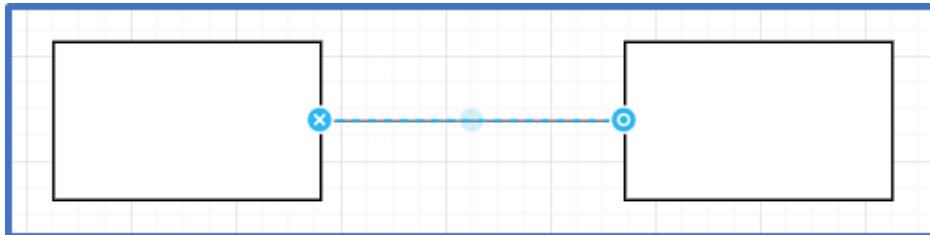


Now go to the toolbar, and select the Waypoints drop down menu. There are different types of connectors that bend at different angles.

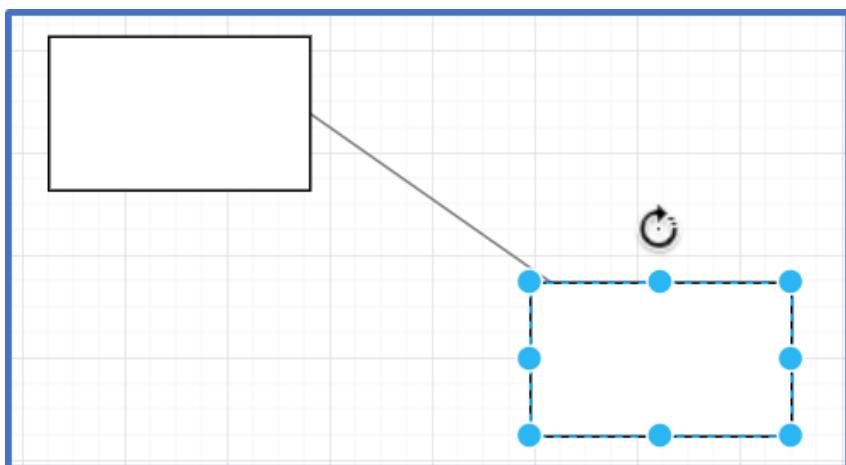


Click the first menu option, Straight (represented by a straight connector) to make the connector a straight line.

The connector is returned to its original path. But now, even though the connector is highlighted, there is no central waypoint. Straight connectors cannot deviate from a straight line, so there is no need for any.

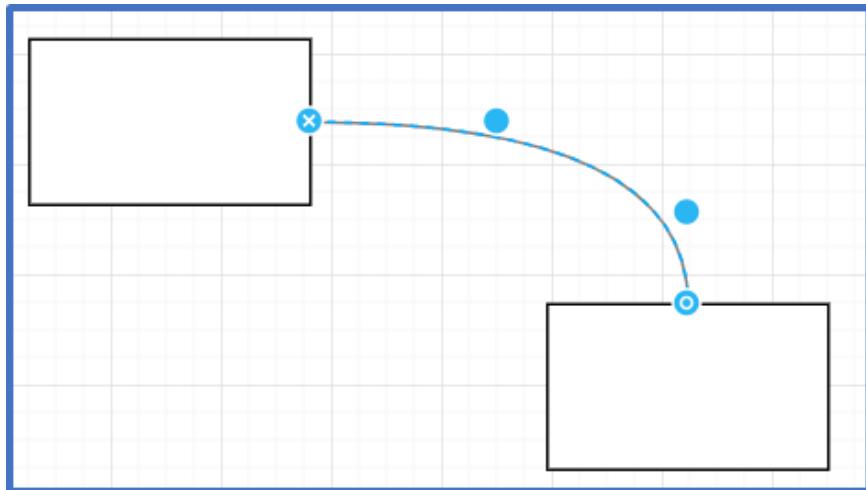


If the second rectangle is moved, the connector will move with it - but it cannot deviate from a straight line.

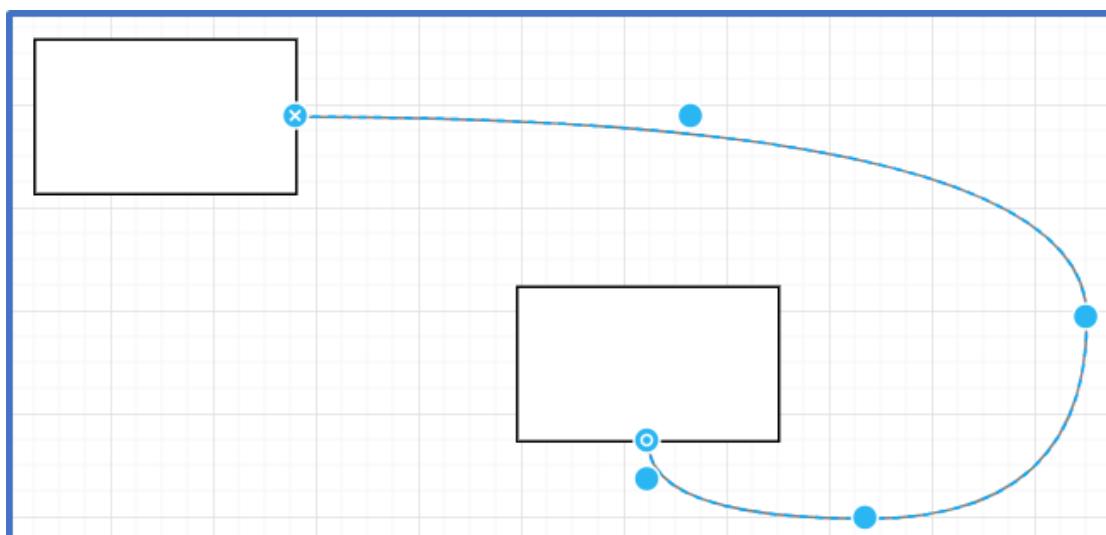
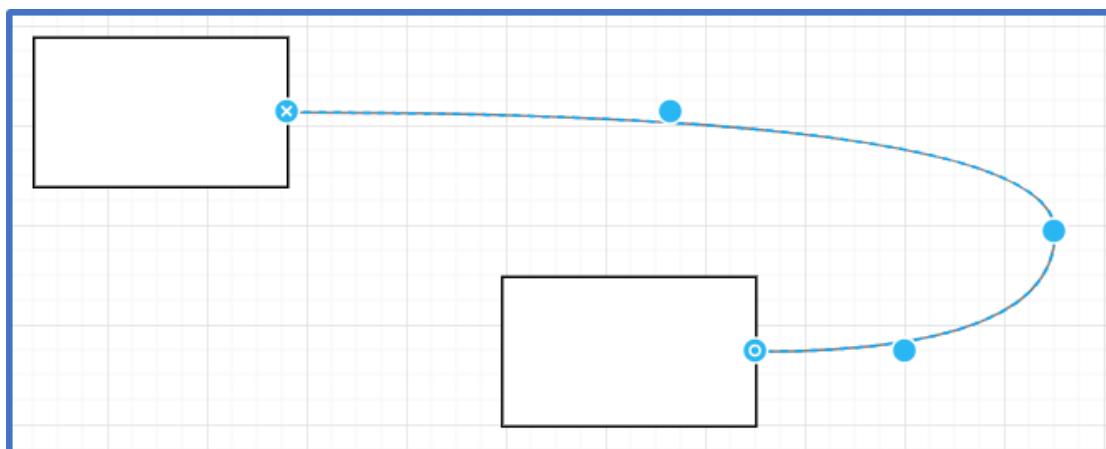


The floating connection to the second rectangle has shifted, as you would expect, but it is no longer attached to any of the connection points on the second rectangle. Contrast this with the default orthogonal connectors, which only travel north, east, south, or west, so even a floating connection will point to the connection points on the edges of the rectangle.

Try a curved connector. From the Connectors menu, select Curved.



Now the connector is curved, and new waypoints have appeared, allowing us to customize the path. It's possible to click and drag a waypoint, just as was seen in the orthogonal example.



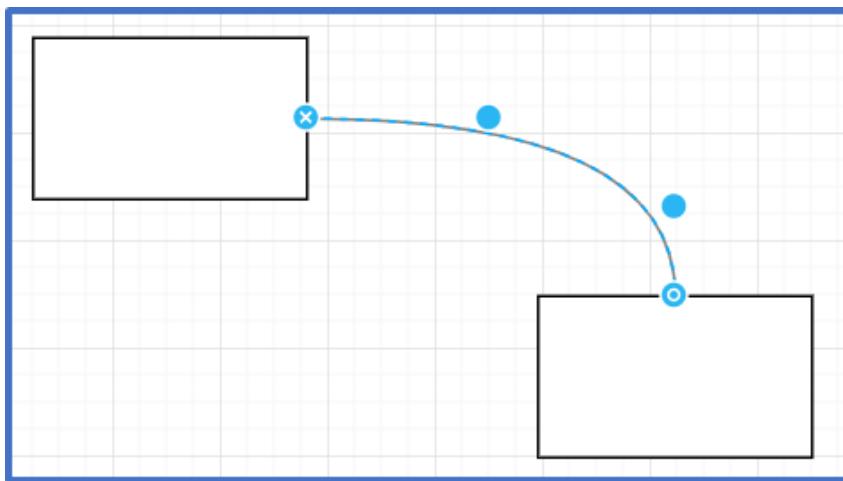
Now there is a new connector path, as well as new waypoints that we have caused to be added.

To conclude, there are a couple of other options available from the right click menu that might be useful. With the connector selected, right click the mouse.

Delete	Delete
Cut	Ctrl+X
Copy	Ctrl+C
Duplicate	Ctrl+D
Set as Default Style	Ctrl+Shift+D
To Front	Ctrl+Shift+F
To Back	Ctrl+Shift+B
Reverse	Ctrl+R
Add Waypoint	
Clear Waypoints	Alt+Shift+C
Edit Data...	Ctrl+M
Edit Link...	Alt+Shift+L

Figure: Right-click menu from connector "Clear Waypoints"

A couple of options relating to waypoints are available. Click Clear Waypoints, and it will remove the waypoints that we added by our manual manipulations. The path changes associated with those waypoints have also been removed. The path has been reverted back to what it was before being manipulated.

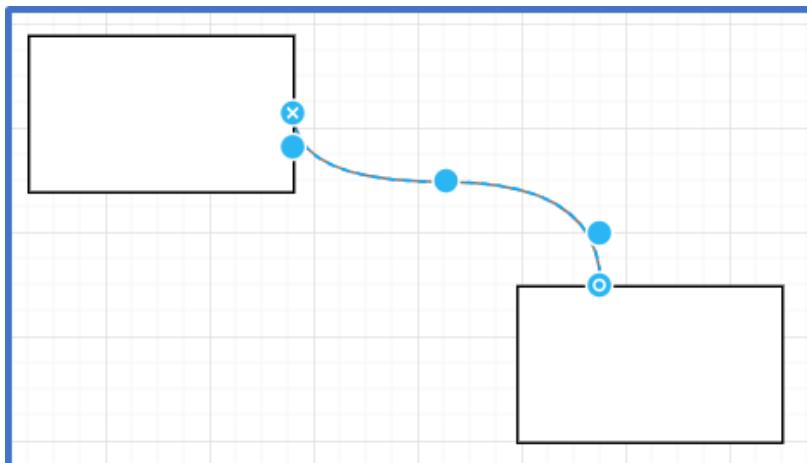


It is also possible to remove the additional waypoints individually, by right clicking on one of them and then selecting Remove Waypoint.

Finally, you can add your own waypoints by right clicking a section of connector where no waypoints currently exist and selecting Add Waypoint.

Delete	Delete
Cut	Ctrl+X
Copy	Ctrl+C
Duplicate	Ctrl+D
Set as Default Style	Ctrl+Shift+D
To Front	Ctrl+Shift+F
To Back	Ctrl+Shift+B
Reverse	Ctrl+R
Add Waypoint	
Clear Waypoints	Alt+Shift+C
Edit Data...	Ctrl+M
Edit Link...	Alt+Shift+L

Figure: Right-click menu from connector "Add Waypoint"



Link Options

When the symbol has been selected, and the Format panel is open on the right-side of the screen you'll see the following options:

Style Tab

Color: As the name implies, this field allows the color of the line to be changed. CSET provides color themes, standard colors, and a form that allows you to create any color, as well as, color opacity.

Geometry: The lines thickness, end decorations, and style are defined by the geometry.

Thickness: Each line in the system can be altered to modify its thickness. Simply enter a number in the field to change its thickness. The Default is 1.

Head and Tail Decorators: This feature allows you to assign an end image, such as a circle, arrow, or diamond, to the head and tail of the line. While this capability is not used often in developing a network diagram, it is available.

Type: Select from the dropdowns to make lines that are straight or wavy.

Text tab

Under the Text tab, the attribute of any embedded text can be changed such as the font, the size, and the text color.

Arrange tab

Under the arrange tab there are options to move front or back, move the connector with the left or top digits, or reverse.

Property tab

Label

Subnet Name: The subnet name is an optional field that is intended for reference purposes only. It is not used in the analysis or reports in CSET. It can be valuable for accurately laying out your network and for design and planning purposes. All subnet-based network analysis is derived from the diagrams zoning configuration.

Security: This field is important for identifying trusted and untrusted lines. An untrusted line may be one where communications are carried, for example, over a public phone line. It could also include internal lines that may cross physical locations that have public access. This field is used in the network analysis. Identifying untrusted lines will also activate network analysis for those lines.

When a line is marked as Untrusted, the system will change the line color to red. This color can be modified if you want to use a different combination of color and thickness.

Link Type: Each link line may be assigned one of five available types. These are for user information only. They do not impact assessment results. New lines are assigned a type of None by default. The available types are:

- Cellular Backhaul,
- Fiber,
- Leased Line,
- Microwave, and
- None.

Adding Text

You may wish to add a title, date, author, or other legend information to better identify the diagram and when and where it was created. Text blocks can also be used to add clarification or descriptive information to specific blocks or areas on the diagram.

Clicking the text tool under the Symbols panel >General tab allows you to create free-form text anywhere on the diagram. Free-form text is text that is not associated with a component. After clicking the button, click in the drawing area where you want the text box to be located. With the mouse button held down, drag the pointer to form a box. Release the mouse button and type the desired text. You can also add text by double clicking anywhere on the diagram.

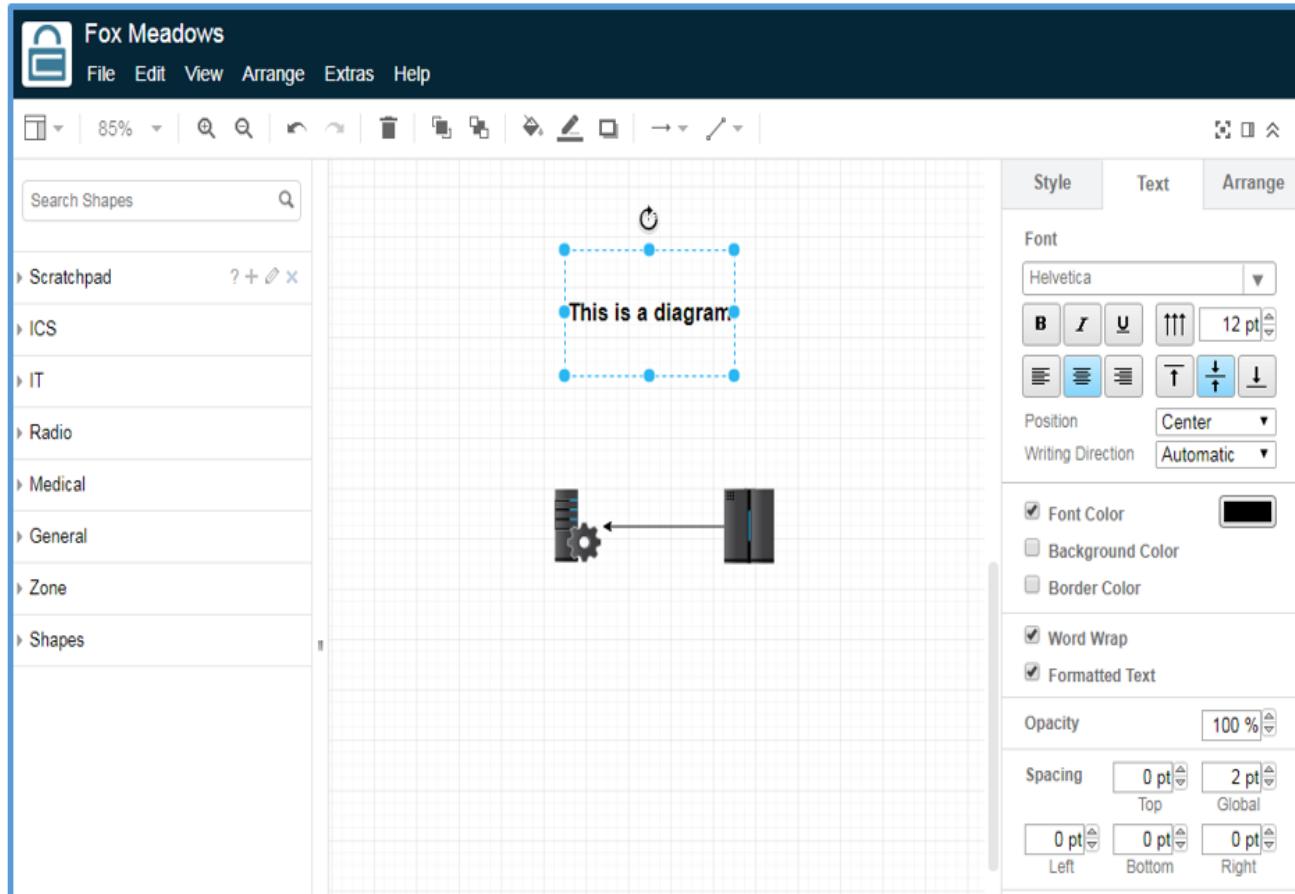


Figure: Text box with panel open

When the text box is selected and the Format panel is open on the right-side of the screen you'll see the following options:

Style tab

Under the Style tab you can add background color, add outline and change the thickness and line type.

Text tab

Under the Text tab, the attributes of the text can be changed such as the font, the size, and the text color.

Continue to add text boxes as needed. Click the Selector tool to stop making text boxes.

Text attributes may also be changed under the Format tab. Double-click on the text to enter edit mode. To see font type, font size, and color changes, click outside of the text box to exit edit mode. Changes may not be visible while in edit mode.

It is possible to paste text into a text box that was copied from another application like Microsoft Word. It is not possible to paste objects like components into a text box.

[Label](#)

[Layer](#)

Arrange tab

The Size tab provides the ability to resize, rotate, and move the text box.

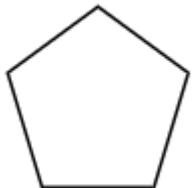
The Property tab is empty for text.

Adding Symbols

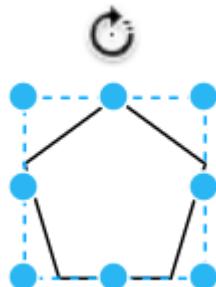
Symbols are the basis of your network diagram. To add a new symbol open the Symbols panel and drag the desired icon onto the drawing area.

Rotating Shapes

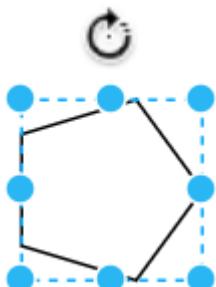
When you create a new shape, it always starts off oriented in some way relative to the page. For example, a pentagon will always appear like this when it is created:



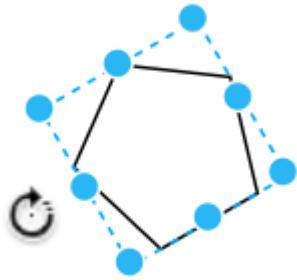
It is possible to rotate any shape, and there are several ways to do this. In order to use any of them, first click on the shape to highlight it.



Notice the curved arrow above the shape. Clicking once on the arrow will rotate the object 90 degrees in a clockwise direction.



Rotation is not constrained to multiples of 90 degrees. By clicking and holding the mouse, and then rotating the cursor left or right, we can rotate a shape in the anti-clockwise or clockwise directions respectively. Below is a pentagon that has been rotated 120 degrees in an anti-clockwise direction.

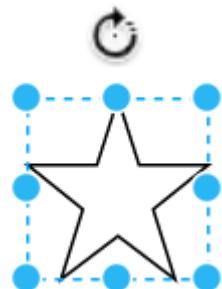


Changing Dimensions

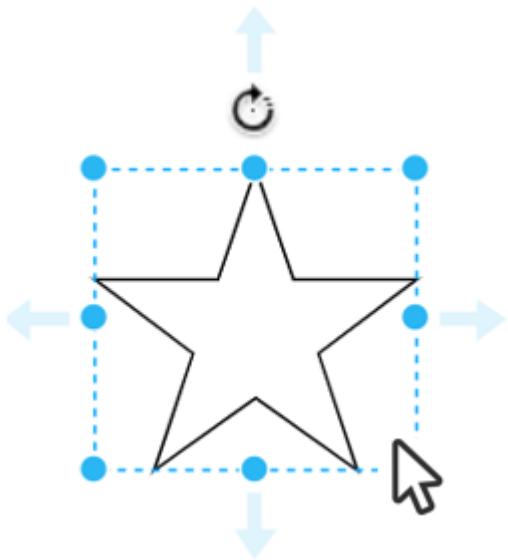
When you create a new shape, it always starts at the same size. For example, a star will always appear like this when it is created:



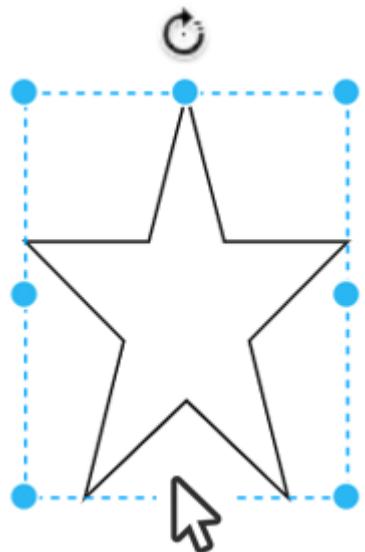
It is possible to resize any shape, and there are several ways to do this. In order to use any of them, first click on the shape to highlight it.



Notice the blue dots around the highlighting frame. By clicking and dragging one of these dots we can resize the shape. Sometimes you will want to preserve a shape's aspect ratio (i.e. keep maintain the same ratio of height to width). To do this, click and drag one of the corner dots.



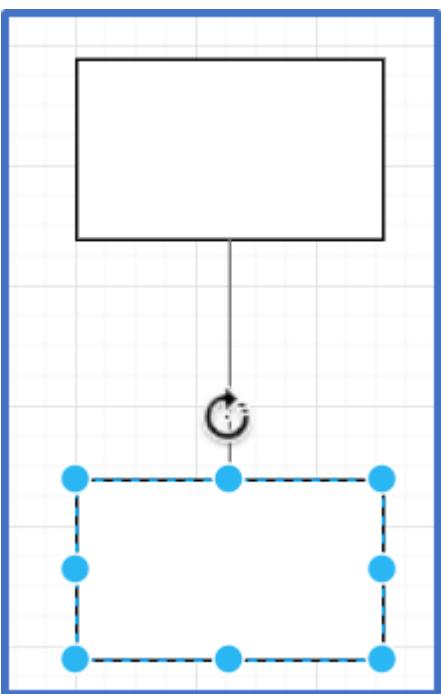
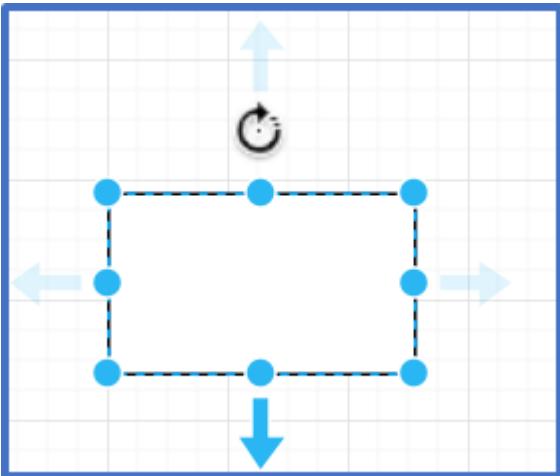
Above the shape is enlarged; it is identical to the original shape but scaled up. You can instead change just the height, or just the width. Do this by dragging on one of the dots on the horizontal lines (to adjust width), or vertical lines (to adjust height).



Above the height of the star is adjusted.

Copy a Symbol

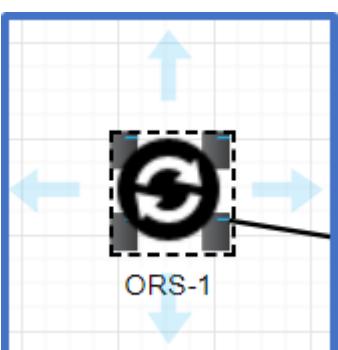
When selecting a shape four blue arrow will appear. Clicking on this will automatically produce a copy of the shape, located in the direction the arrow points.



You can also copy symbols, links, text, etc. by using the shortcut **Ctrl+C** (**CMD +C** for Mac) or **Copy** from the **Edit** menu.

Replace a Symbol

Sometimes we want to replace one shape in a diagram with another one. Start by clicking and dragging a symbol over one of the items on your diagram, until you see the following:



This indicates that you can replace the old shape with the new one. Simply release the new symbol and it will appear on the diagram.

Add a Symbol to a Pre-existing Connector

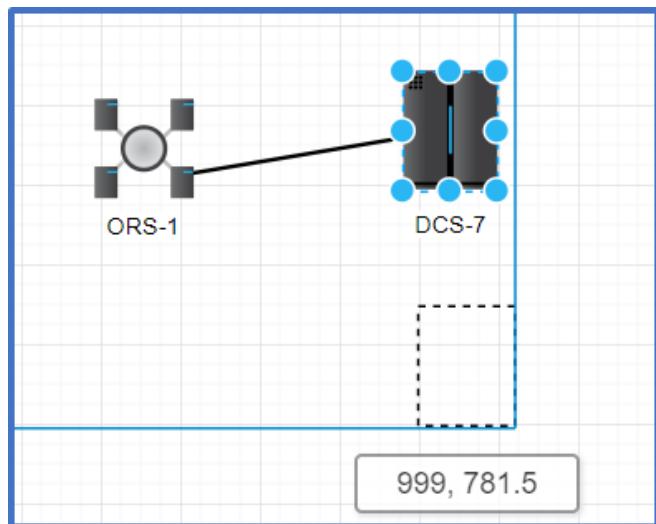
Create a connector from any symbol (This is explained in the [Adding Links](#) help section).

With the new connector still highlighted, go to the Symbol panel and click on any shape.

The new shape appears and is automatically connected to the other end of the highlighted connector.

Move Symbols

You might decide that we don't want a symbol where CSET initially placed it. Since the shape is already have the shape highlighted, drag it somewhere else.

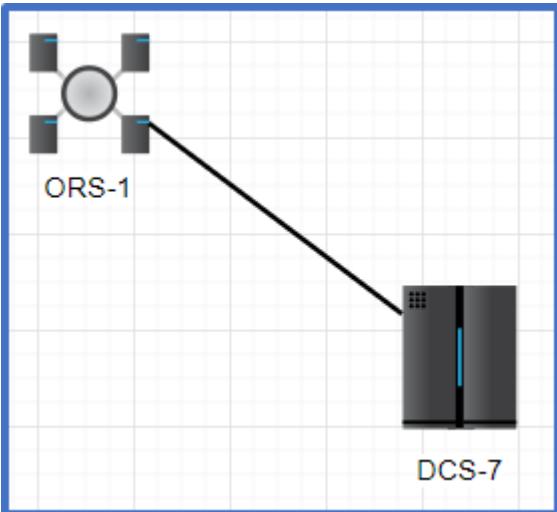


DCS-7 is in its original position, but it hasn't been released yet. As we move the shape, CSET provides information that helps us to place it where you want.

First, there is a dotted outline showing where the shape would go if it is released in its current position. It also provides the current coordinates for that position, taken from the top left of the shape. And sometimes you will see blue guidelines appearing. These indicate that an edge or central axis of the shape are aligned to the edge or central axis of another nearby shape. In the above example, you can see that our current position is aligned with two shapes, one vertically, and one horizontally.

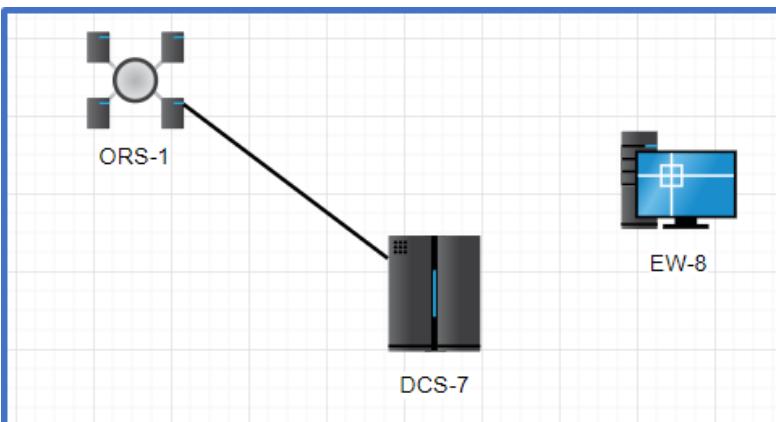
Drop the shape here, and click once, away from the shape, so that it is no longer highlighted.

The shape appears in its new position, and the connector has altered its course so that it remains connected. It is now connected to a point at the top left corner of DCS-7. This is handled by CSET automatically for any floating connection.

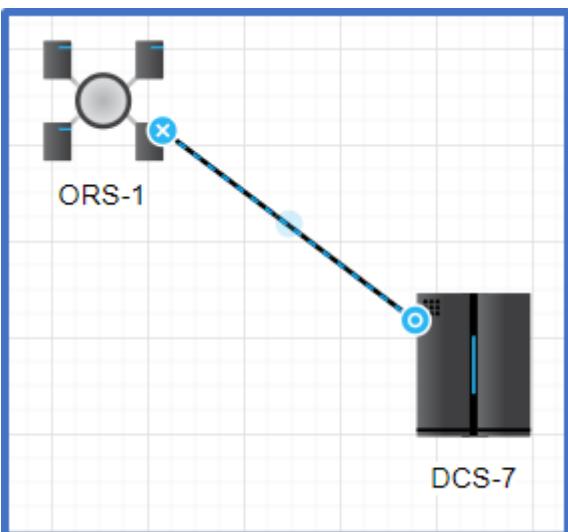


Change a Connection

Sometimes you will want to change the connections in the diagram. Perhaps the connection to DCS-7 needs to be to another symbol instead. Start by dragging any new item from the Symbol panel onto the diagram.

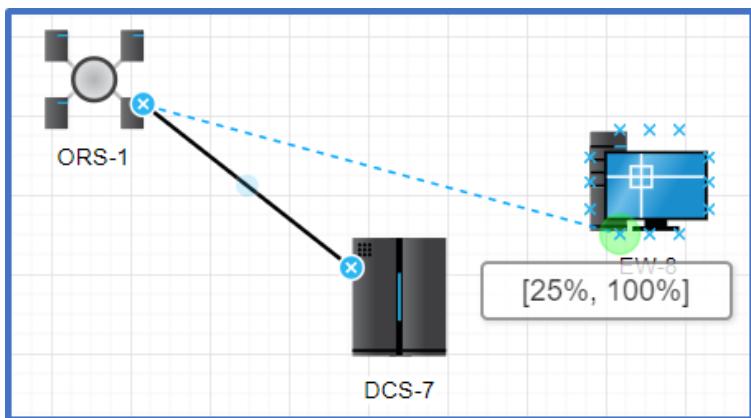


Move the arrow end of the connector so that it connects to EW-8. It is connected to DCS-7 and will move that item. To move the connector, first highlight it and then place the cursor over the connector arrow.



Now click and drag the arrow over to EW-8. If you want to connect and anchor the connector to a point, you will need to find one of the connection points around the perimeter. Connection points are usually located at regular intervals around a shape, often where an axis of symmetry intersects with the perimeter.

You will know when you have dragged the connector over one of the connection points, because all the connection points will appear, and the one you are currently hovering over will be surrounded by a small green circle, indicating that the connector is correctly placed to connect to this point.



Releasing the connector will connect and anchor it to EW-8. If the symbol is moved, the connector will follow it.

Symbol Properties

When the symbol has been selected, and the Format panel is open on the right-side of the screen you'll see the following options:

Style tab

Under the style tab the you can select color to fill the shapes, line width and color, opacity and other effects like rounded, glass, shadow and comic.

Text tab

Under the Text tab, the attributes of the shape's text can be changed such as the font, the size, and the text color.

Arrange tab

The Size tab provides the ability to resize, rotate, and move the shape.

Property Tab

Note: The Property tab is only available for CSET icons.

[Label](#)

[SAL](#)

[IP Address](#)

[Asset Type](#)

[Criticality](#)

[Host Name](#)

[Has Unique Questions](#)

[Description](#)

Adding Zones

A zone is a visual representation on the diagram of a physical or logical boundary separating different functional areas. It could also be used to represent systems that are bordered by physical structures such as a fence, building, rooms in a building, or even a plant. A common example is the separation of a corporate information system and an industrial control system (ICS). These two networks could be miles apart or all located at the same facility.

The advantage to using zones is that you are able to provide the appropriate level of security for both the highly critical areas and those that have little consequence. An area in the plant that has very high risk may be secured to a level of Very High, while much of the plant or organization may be at a Moderate or even Low level. This can be helpful when resources are limited, and you need to know where to spend your time, energy, and budget.

To create a zone in CSET, you will need to click the Zones pane on the Symbols panel.

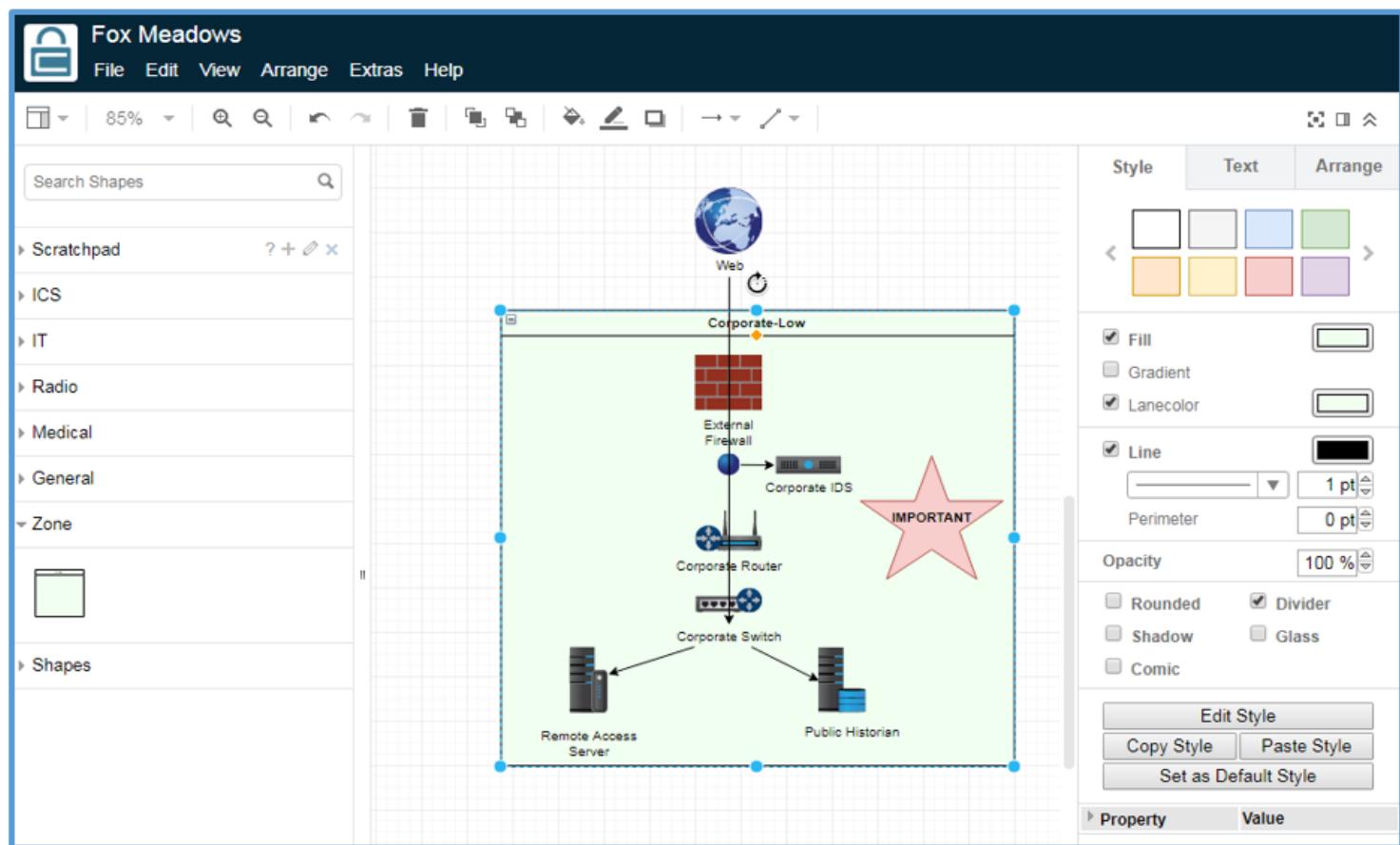


Figure: Adding a zone

Drag a zone onto the drawing area. The zone will be initially placed as a blank rectangle. Drag the corners of the zone to include the desired components. If in doubt, place the zone first then add the components and links. The zone will expand to accommodate newly placed components that are at least halfway into the zoned area.

Moving a zone and dropping it onto an existing component will cause that component to become part of the zone and move with it. Components already assigned to another zone may be incorporated in this way. Caution must be used because unwanted components can be captured and inadvertently included in the wrong zone. It is recommended that components be added individually to zones, rather than collecting them by dragging and dropping the zone onto them.

Zone Properties

When the symbol has been selected, and the Format panel is open on the right-side of the screen you'll see the following options:

Style tab

Under the style tab the you can select color to fill the zone and lane color, line width and color, opacity and other effects like rounded, glass, shadow and comic.

Text tab

Under the Text tab, the attribute of any embedded text can be changed such as the font, the size, and the text color.

Arrange tab

The arrange tab provides the ability to resize, rotate, and move the zone.

Properties tab

Label

Type: The type field provides a list of general categories of systems, including Other. Each type has a predefined SAL and associated color. Once you select a type, it will fill in the zone and give it a default label.

SAL

Owner: The Owner field allows for the identification of the person in charge of or responsible for the zone and its included components.

Note: All properties are for the zones themselves, not for the items inside them.

Using the Multiple Services Component (MSC)

When multiple icons are needed to represent a single physical device, such as a firewall and IDS, the Multiple Services Component (MSC) may be used to group the icons. Like the Zone icon, the MSC icon is essentially a boundary or border with which to enclose the components. Clicking the MSC displays the Format panel on the right-side of the screen.

Add an MSC to a Diagram

To use the icon, select it from the ICS Component window and drag it onto the drawing area.

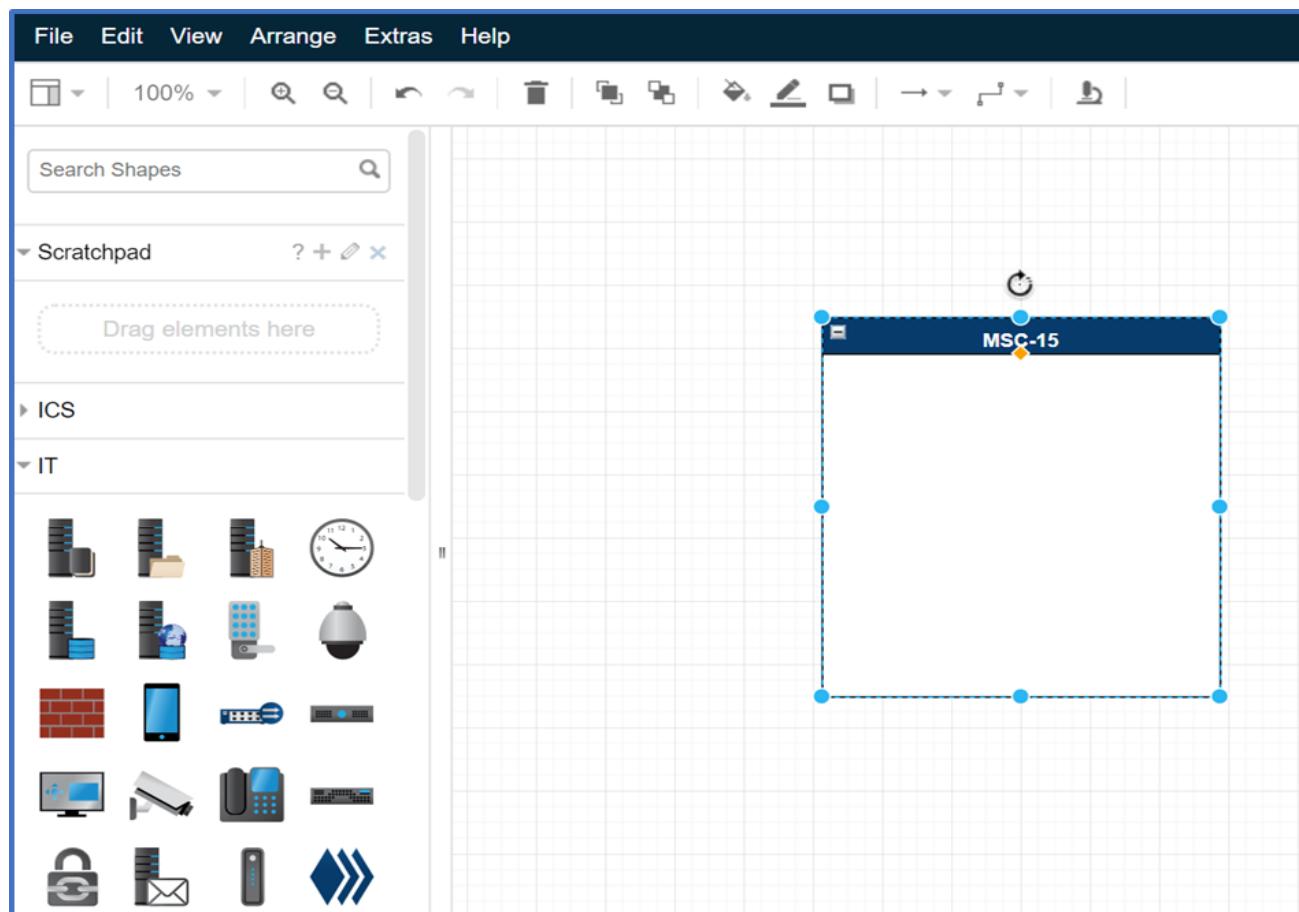


Figure: Adding an MSC

MSCs behave like other symbols. You can add links and connect them to other zones and shapes.

Clicking the minus at the upper left corner of the MSC icon will collapse the icon to save drawing space. Restore the icon to normal size by clicking the plus sign.

In the Assessment Analysis and Reports, the MSC will not be shown. Instead, each included service will be listed individually. The default tags include the MSC designation then the service abbreviation. For example, an application server within Multiple Services Component 1 (MSC-1) will be labeled MSC-1-AS-x where x is a sequential number. The default tag can be changed by double-clicking in the tag field.

Adding a Symbol to an MSC

Add as many symbols as desired to the MSC by dragging them onto the shape. The MSC will highlight in purple when the symbol can be released and added. The figure below shows a symbol being added to an MSC.

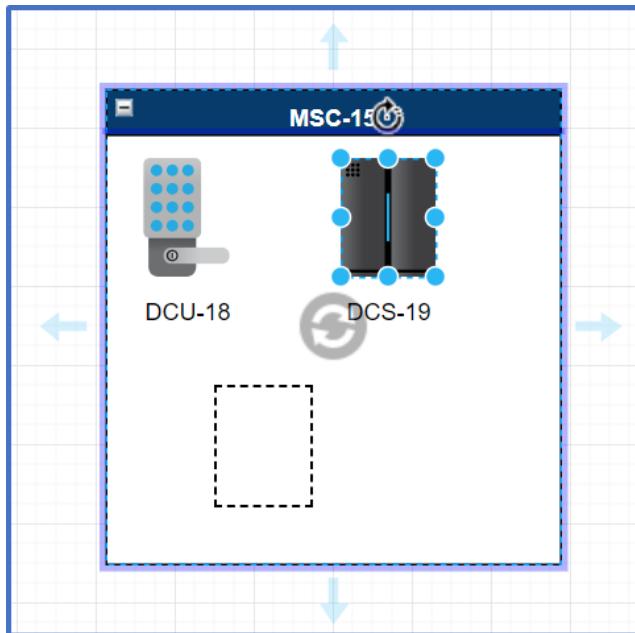


Figure: Adding a symbol to an MSC

The gray circle icon in the middle of the MSC behaves like described in the help section [Adding Symbols](#). It will replace the entire MSC with the shape you are dragging on to it.

The MSC needs to be resized manually to accommodate more symbols than will fit the initial size. For resizing symbols read the help section for [Adding Symbols](#).

MSC Options

Clicking on the MSC will open the Format panel on the right-side of the screen.

Style tab

Under the style tab the you can select color to fill the zone and lane color, line width and color, opacity and other effects like rounded, glass, shadow and comic.

Text tab

Under the Text tab, the attribute of any embedded text can be changed such as the font, the size, and the text color.

Arrange tab

The arrange tab provides the ability to resize, rotate, and move the zone.

Property tab

Label

SAL: The SAL for an MSC is read-only. See [SAL](#) for more information.

IP Address

Asset Type

Criticality

Host Name

Has Unique Questions

Description

Component Types

The table below presents a list of the Components currently available in CSET with a brief description of their use.

CSET Type	Brief Description
Active Directory	A directory service that Microsoft developed for Windows domain networks and is included in most Windows Server operating systems
Application Server	A computer used to control distribution of a computer application to one or more users
Audio Switch	Is a component that has the capability to digitize audio and send to other network paths. This component will be used in connection to a PBX, dispatch operator or some audio source.
Building Automation Management Systems	A computer-based control system installed in buildings that controls and monitors the building's mechanical and electrical equipment such as ventilation, lighting, power systems, fire systems, and security systems.
Clock	A timing device coordinated for accuracy to a GPS, CDMA, or time server used by the control system
Configuration Server	A server that either is used to store control system component configurations and/or actively pushes and pulls configuration from control system components.
Connector	A logical (not physical) node that allows network lines to be shown as connected
CT Scanner	A device that uses x-ray computed tomography (X-ray CT) or computerized axial tomography (CAT) that makes use of computer-processed combinations of many X-ray images taken from different angles to produce cross-sectional (tomographic) images (virtual 'slices') of specific areas of a scanned object, allowing the user to see inside the object without cutting).
DB Server - Database Server	Server managing relational database table data, most commonly for a historian
DCS - Distributed Control System	System used to remotely monitor and control distributed equipment
Dispatch Console	A component that represents equipment used by dispatchers whom are responsible for receiving and transmitting pure and reliable messages, tracking vehicles and equipment, and recording other important information.
Domain Name System Server	A (DNS) System for converting alphabetic names into numeric IP addresses.
Door Access Door Control Unit	The most common used system in electronic door control using a card or a magnetic stripe which can be accessed by swiping through a reader on the door. These access control systems are used for security purposes.
Electrocardiograph	An ECG is a simple, noninvasive procedure. Electrodes are placed on the skin of the chest and connected in a specific order to a machine that, when turned on, measures electrical activity all over the heart. Output usually appears on a long scroll of paper that displays a printed graph of activity on a computer screen.
Electroencephalograph	An electroencephalogram (EEG) is a test that detects electrical activity in your brain using small, flat metal discs (electrodes) attached to your scalp. Your brain cells communicate via electrical impulses and are active all the time, even when you're asleep.
Electromyograph	Electromyography (EMG) is a diagnostic procedure to assess the health of muscles and the nerve cells that control them (motor neurons). Motor neurons transmit electrical signals that cause muscles to contract.

Electronic Security System	Refers to any electronic equipment that could perform security operations like surveillance, access control, alarming or an intrusion control to a facility or an area which uses a power from mains and also a power backup like battery etc.
Email Server	Is a server that handles and delivers e-mail over a network, usually over the Internet. An e-mail server can receive e-mails from client computers and deliver them to other mail servers. An e-mail server can also deliver e-mails to client computers. A client computer is normally the computer where you read your e-mails, for example your computer at home or in your office. Also an advanced mobile phone or Smartphone, with e-mail capabilities, can be regarded as a client computer in these circumstances.
Emergency Medical Service Communications Hardware	In most places in the world, the EMS is summoned by members of the public (or other emergency services, businesses, or authorities) via an emergency telephone number which puts them in contact with a control facility, which will then dispatch a suitable resource to deal with the situation. The Emergency Medical Service Communications Hardware consists of dispatch panel, radios, and cellular devices used by medical personnel to communicate with personnel in the field, or locally within a medical campus.
Endoscopy System	Device used to look inside the body for medical reasons
EWS - Engineering Workstation	Computer that the process control engineer uses for technical support of control systems
Ethernet Backhaul	is a communication element that transmit data from the central system to edge nodes of a communication system. The first part of the name indicates the physical method used to transmit data.
FEP - Front End Processor	Device to handle communications to peripherals on behalf of the main processor
Firewall	Hardware and/or software used to prevent communications not authorized by the security policy
Handheld Wireless Device	A wireless device in a hand-held form factor
Historian	Operational historian refers to a complementary set of time-series database applications that are developed for operational process data. Historian software is often embedded or used in conjunction with standard DCS and PLC control systems to provide enhanced data capture, validation, compression, and aggregation capabilities. Historians have been deployed in almost every industry and contribute to functions such as supervisory control, performance monitoring, quality assurance, and, more recently, machine learning applications which can learn from vast quantities of historical data. Raw data may be accessed via OPC HDA, SQL, or REST API interfaces.
HMI - Human-Machine Interface	A display that shows control system status/alarms, usually generated by an application server
Hub	A device to connect separate lines of a network together
IDS - Intrusion Detection System	System that detects unauthorized or malicious access to a computer system or network
IED - Intelligent Electronic Device	Microprocessor-based controller of power system equipment.
Imaging Modalities and Equipment	Medical imaging is the technique and process of creating visual representations of the interior of a body for clinical analysis and medical intervention, as well as visual representation of the function of some organs or tissues (physiology). Medical imaging seeks to reveal internal structures hidden by the skin and bones, as well as to diagnose and treat disease. Medical imaging also establishes a database of normal anatomy and physiology to make it possible to identify abnormalities. Although imaging of removed organs and tissues can be

	performed for medical reasons, such procedures are usually considered part of pathology instead of medical imaging
Imaging Server	Most medical imaging devices require some form of image storage and computing support. Imaging servers are the general class of imaging storeage or computing and support devices.
Infant Protection Remote Display Unit	An Infant Protection System provides hospital-wide protection against infant abduction and mother/infant mismatches, with each infant individually protected by multiple layers of security.
Intelligent Embedded Device	Is characterized as the ability of a product, process or service to reflect on its own operational performance, usage load, or environment to enhance the product performance and lifetime, to increase quality or to ensure customer satisfaction. This self-reflection, facilitated by information collected by embedded sensors, processed locally or communicated remotely for processing, must be considered from the earliest design stage.
Interactive Television System	Interactive television is a form of media convergence, adding data services to traditional television technology. Throughout its history, these have included on-demand delivery of content, as well as new uses such as online shopping, banking, and so forth.
IP Camera - Internet Protocol Camera	A type of digital video camera commonly employed for surveillance that can send and receive data via a computer network and the Internet.
IP Phone - Internet Protocol Phone	A telephone that can transmit audio over the internet
IPS - Intrusion Prevention System	System that detects and filters unauthorized or malicious access to a network
IV Infusion Pump	An infusion pump is a medical device that delivers fluids, such as nutrients and medications, into a patient's body in controlled amounts. Infusion pumps are in widespread use in clinical settings such as hospitals, nursing homes, and in the home.
Linear Particle Accelerator	Device that generates X-rays and high energy electrons for medicinal purposes in radiation therapy.
Link Encryption	A device providing bulk encrypting of all traffic passed via a link
Magnetic Resonance Imaging Equipment	Test that uses a magnetic field and pulses of radio wave energy to make pictures of organs and structures inside the body
Master Site	A component to represent the general core radio system equipment that performs the control of radio transmissions and also interconnects to other radio system domains.
Medical Piped Gas Supply System	Medical piped gas systems in hospitals, and most other healthcare facilities, are essential for supplying piped oxygen, nitrous oxide, nitrogen, carbon dioxide and medical air to various parts of the hospital. These systems are usually highly monitored by various computerized alarm systems.
Microwave Backhaul	A communication element that transmit data from the central system to edge nodes of a communication system. The first part of the name indicates the physical method used to transmit data.
Modem	A device that modulates/demodulates an analog signal to encode digital information for transmission over a public switched telephone network (PSTN)
MTU - Master Terminal Unit	A device that collects and disperses data between a SCADA system and Remote Terminal Units (RTU)
Multiple Services Component	A single network component that may be assigned to many services.

Multi-Protocol Label Switching	Is a routing technique in telecommunications networks that directs data from one node to the next based on short path labels rather than long network addresses, thus avoiding complex lookups in a routing table and speeding traffic flows.
Network Printer	Printer that is connected directly to the network
Network Scanner And Copier	is an IP scanner that is used for scanning both large corporate networks that have hundred thousands of computers along with small home networks with several computers.
Optical Ring (Sonet Device)	A device providing access to the Sonet Ring
Optical Ring System	An optical ring resonator is a set of waveguides in which at least one is a closed loop coupled to some sort of light input and output. (These can be, but are not limited to being, waveguides.)
Partner	Represents a connection to a company partner
PC - Personal Computer	A microcomputer designed for use by one person at a time
Physiological Monitoring System	In medicine, monitoring is the observation of a disease, condition or one or several medical parameters over time. It can be performed by continuously measuring certain parameters by using a medical monitor (for example, by continuously measuring vital signs by a bedside monitor), and/or by repeatedly performing medical tests (such as blood glucose monitoring with a glucose meter in people with diabetes mellitus). Examples of possible monitoring systems include: Cardiac monitoring, Hemodynamic monitoring, Respiratory monitoring, Capnography, Neurological monitoring, Blood glucose monitoring, or Childbirth monitoring.
PLC - Programmable Logic Controller	Small programmable device for managing and collecting data from end devices
Power Over Ethernet	Describes any of several standard or ad-hoc systems which pass electric power along with data on twisted pair Ethernet cabling. This allows a single cable to provide both data connection and electric power to devices such as wireless access points, IP cameras, and VoIP phones.
Public Kiosk	Is a computer terminal featuring specialized hardware and software that provides access to information and applications for communication, commerce, entertainment, or education.
Radio Site	is a component that represents a remote located radio tower. It can contain subelements (such as antennas, power systems, backhauls, etc.) Other components can be colocated along with the radio tower if desired.
RAS - Remote Access Server	Server managing remote access to intranet components
Real Time Location System	Real-time locating systems (RTLS) are used to automatically identify and track the location of objects or people in real time, usually within a building or other contained area. Wireless RTLS tags are attached to objects or worn by people, and in most RTLS, fixed reference points receive wireless signals from tags to determine their location. Examples of real-time locating systems include tracking automobiles through an assembly line, locating pallets of merchandise in a warehouse, or finding medical equipment in a hospital. The physical layer of RTLS technology is usually some form of radio frequency (RF) communication, but some systems use optical (usually infrared) or acoustic (usually ultrasound) technology instead of or in addition to RF. Tags and fixed reference points can be transmitters, receivers, or both, resulting in numerous possible technology combinations.
Relay Panel	is a component that represents a device to transmit T1 data to other T1 nodes and acts as a router.

RFID Transmitter	Uses electromagnetic fields to automatically identify and track tags attached to objects. The tags contain electronically stored information. Passive tags collect energy from a nearby RFID reader's interrogating radio waves. Active tags have a local power source (such as a battery) and may operate hundreds of meters from the RFID reader. Unlike a barcode, the tags don't need to be within the line of sight of the reader, so it may be embedded in the tracked object. RFID is one method of automatic identification and data capture.
Router	A computer networking device that forwards data packets to its destinations between disparate networks
RTU - Remote Terminal Unit	A device that interfaces objects to a DCS or SCADA system by transmitting telemetry data
Security Information and Event Management System	In the field of computer security, security information and event management (SIEM), software products and services combine security information management (SIM) and security event management (SEM). They provide real-time analysis of security alerts generated by applications and network hardware.
Serial Radio	A device providing modem functionality for use over wireless links
Serial Switch	A device providing automatic or manual switching between serial devices
Server	A generic term for a computer that provides data to other computers
SIS - Safety Instrumented System	An engineered set of hardware and software control especially used on critical process systems. The combination is treated as a single component
Subscriber Radio	A component representing a mobile land radio device. A wireless communication system intended for use by users in mobile vehicles or on foot. Examples of these devices are a handset, car installed unit, or radio connected computer terminal.
Switch	A network device that connects computer devices in a network (sometimes referred to as a Managed Switch)
T1 Backhaul	A communication element that transmit data from the central system to edge nodes of a communication system. The first part of the name indicates the physical method used to transmit data.
TDM Backhaul	A communication element that transmit data from the central system to edge nodes of a communication system. The first part of the name indicates the physical method used to transmit data.
Terminal Server	A device providing protocol encapsulation of serial data via a network
Ultrasound	A diagnostic imaging device based on the application of ultrasound. Used to see internal body structures such as tendons, muscles, joints, vessels and internal organs.
Unidirectional Device	Allows data to travel only in one direction (i.e., corporate network to control system network)
Uninterruptible Power Supply	Is an electrical apparatus that provides emergency power to a load when the input power source or mains power fails.
Unknown	Icon to represent a component type not already available in the CSET shape list
Urodynamic Diagnostic Equipment	Systems designed to measure and evaluate the storage and transportation of urine in the urinary tract. These systems consist of a set of units that are combined to perform all the measurement functions as well as display and recording devices. The systems include uroflowmeters and uroflow transducers for external measuring of the urinary flow, volume voided, peak flow, and voiding time; manometers to determine the urethral pressure profile; cystometers either liquid or gaseous to measure bladder capacity and response; and recorders with appropriate sensors to assess sphincter and other muscle activity. Many systems also include video

	urodynamics capabilities to allow radiographic and urodynamic studies to be performed with synchronous display and recording of urodynamic studies and cystourethrography imaging. Urodynamic measuring systems are used in diagnosing neurogenic bladder diseases, stress incontinence, urinary path obstructions, and spastic sphincters.
Vendor	Represents a connection to an external vendor
Video Teleconferencing Equipment	Video conferencing is a technology that allows users in different locations to hold face-to-face meetings without having to move to a single location together. There are a variety of ways video conferencing can be conducted. Individuals may use web cameras connected to our built into laptop, tablet, or desktop computers. Smartphones equipped with cameras may also be used to connect for video conferences. In such instances, a software-based platform typically is used to transmit the communication over Internet protocols. Some businesses use dedicated video conferencing rooms that have been equipped with high-grade cameras and screens to ensure the conversation is clear and with limited technical faults. Third-party providers often install and assemble the hardware needed to conduct the video conference.
Virtual Machine Server	A component that represents a server that hosts multiple virtual machines running operating systems in a fully virtual (completely emulates all hardware devices) or para-virtual mode (complete emulation of hardware devices is not required).
VLAN Router - Virtual Local Area Network Router	A networking device that forwards data packets between standard or virtual subnets
VLAN Switch - Virtual Local Area Network Switch	A network device that connects computer devices in a network, handling multiple subnets
VPN - Virtual Private Network	A software tunnel used for secure communications over a public network
Web	A symbol to represent the part of the network that is accessible to the public
Web Server	Server used to store and manage access to web pages and applications
Windows Update Server	Windows Server Update Services, previously known as Software Update Services, is a computer program and network service developed by Microsoft Corporation that enables administrators to manage the distribution of updates and hotfixes released for Microsoft products to computers in a corporate environment.
Wireless Modem	A modem that bypasses the telephone system and connects directly to a wireless network
Wireless Network	Communication device that exchanges data with other wireless components using radio signals
Wireless Router	A component which represents a device that performs the functions of a router and also includes the functions of a wireless access point.
XRay Generator	Uses x-ray light to view the internal structure of a non-uniformly composed and opaque object such as the human body.

Table: Valid Component Types

The following Components have no associated questions. Therefore, they are not included in the analysis of assessment compliance.

- Connector,
- Hub,
- Multiple Services Component (with no included services),

- Unknown,
- Web, and
- Zone (with no included components).

Home Menu Options

The Home menu is divided into File, Edit, View, Arrange, Extras, and Help. Below is an explanation of all the menu items.



Figure: Home menu options

Home- File Menu

The functions under the File menu are:

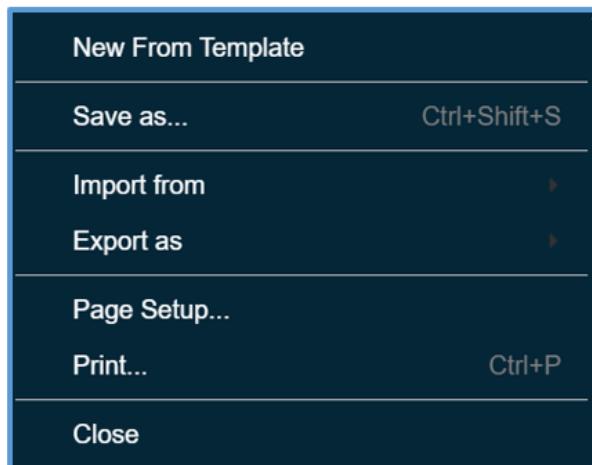


Figure: Diagram file menu

New from template: New from template opens the CSET template dialogue (the same dialogue that opens with each new diagram). You can pick out of the pre-installed templates that are included with CSET. These are basic configurations that are somewhat unique to a given sector or system type. They are intended to provide a starting point for building a diagram specific to your system.

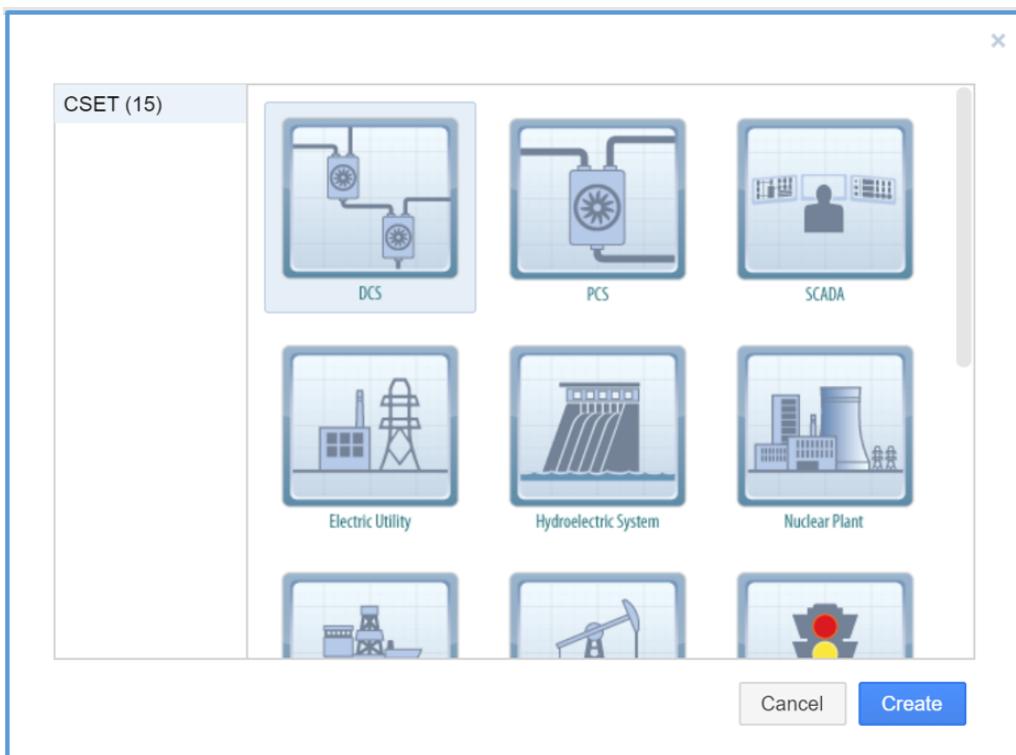


Figure: New from template dialogue

Remember that if you load a new template, the system will clear or wipe away what is currently there. The answers to any questions related to components will be lost as will the diagram itself. If you want to save just the diagram without saving answers, use the Export Diagram function.

Save as: Allows the user to name, locate, and save the file.

Import from: Import from will import from a .csetd file.

Export as: Export as: Export as will export the diagram as a .png, .jpeg, .svg, or .vsdx. The diagram can be exported as a PDF by printing the diagram and selecting the print destination as “Save as PDF” instead of a printer. There are advanced options that the user can use to pick export type, zoom, height, width, transparency, and border width.

Page setup: Page setup provides options for paper size, orientation, background, and image.

Print: Print has option for adjust to %, fit to sheet, paper size, orientation, scale to %, and preview.

Close: Will close the diagram.

Home- Edit Menu

The functions under the Edit menu are:

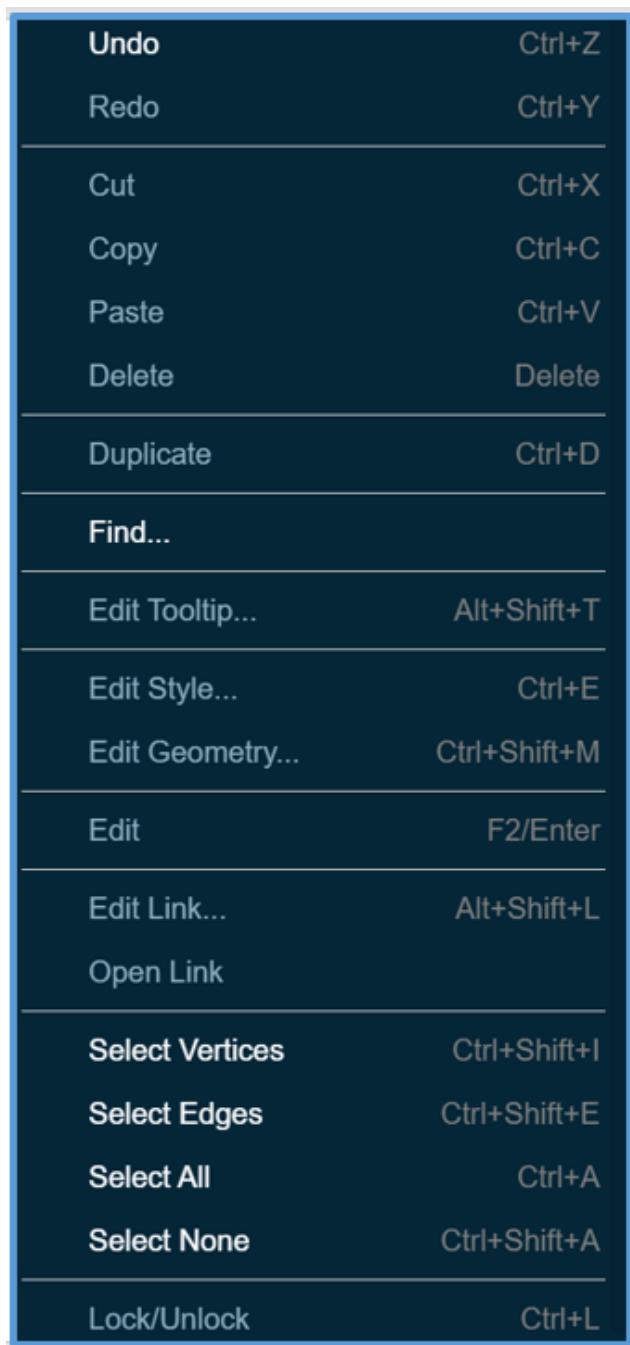


Figure: Diagram edit menu

NOTE: Any time a component is removed from the diagram, whether by Cut or Delete, any questions associated with the component are removed from the assessment in real time. The removal cannot be undone. If a component is removed and re-added, any previous answers associated with that component will need to be provided again.

Undo: This key will reverse a previous change, such as the movement of an object or a deletion. This function does not undo every action that was issued, but it does cover most of the commands.

Redo: The Redo button will reverse most of the Undo changes. The combination of Undo and Redo involve buffering a set of actions. The Undo reverses the buffered change, and the Redo reissues the command. Both Undo and Redo have limitations in terms of the number and types of action performed.

Cut: This function allows you to select an object, such as a line or component, and then click on the Cut button to remove the object from the diagram. The Cut option is slightly different than the Delete button in that the cut method will hold a copy of the object for pasting whereas the Delete option will simply remove the object.

Copy: The copy button allows you to select an object from the diagram and then have it available to paste. The Paste icon is no longer grayed out when the object has been copied. Multiple objects can be copied at one time using the block selection function.

When you copy and paste a component, the name will remain the same, as will all the other properties. A copied component or set of components is created slightly offset from the original. Remember to change the name to something unique after you have created it.

You can also use the familiar Ctrl-C keyboard combination to copy a selected object with the tool. You cannot copy objects from CSET and paste them into other applications. Attempting to do so will produce useless metadata in the new application if it pastes anything at all.

Paste: Paste is a familiar action for most computer users and will make a copy of the selected objects that have been cut or copied. When they are created, they will be in a selected state and slightly offset from the original. While in this state, they can be moved to a new location on the diagram. You can use the Ctrl-V combination to paste the objects that have been cut or copied.

You cannot place non-CSET objects onto the diagram using the Paste command. For example, you may want to place a logo on the diagram or even a text string, but the tool will only allow objects that are native to CSET to be inserted into the diagram. It will not use the contents of the Windows Clipboard.

Delete: The Delete command behaves much like the Cut command. The difference is that it does not perform an associated copy. The Delete key from the keyboard will also remove the selected object or text string.

Duplicate: Duplicate creates an instant copy of whatever symbol/link you have highlighted and pastes it on your diagram.

Find: By typing into the Find dialog, any shapes with a label or metadata matching the entered search term will be selected. Clicking the Find button or pressing ENTER will select the next matching entry (or select the first entry if no more entries are found).

Checking "Regular Expression" will allow regular expression in the JavaScript syntax to be used for the search term.

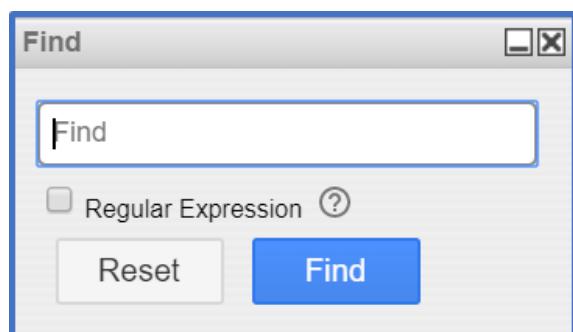


Figure: Find dialogue

Edit tooltip: Edit tooltip will bring up a textbox to enter a tooltip for the symbol highlighted.

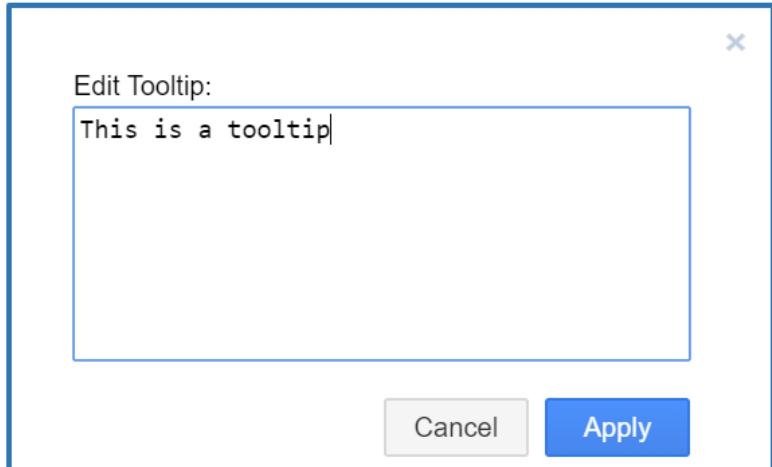


Figure: Editing a tooltip

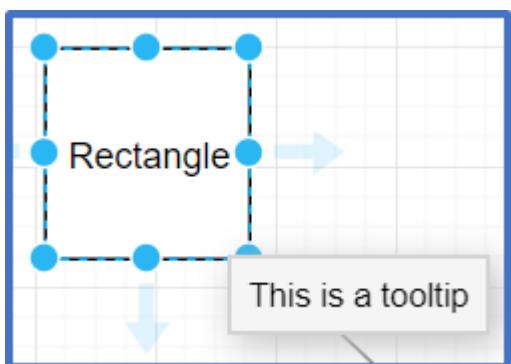


Figure: Shape with the tooltip active

Edit style: Edit style allows you to edit the style of a highlighted symbol.

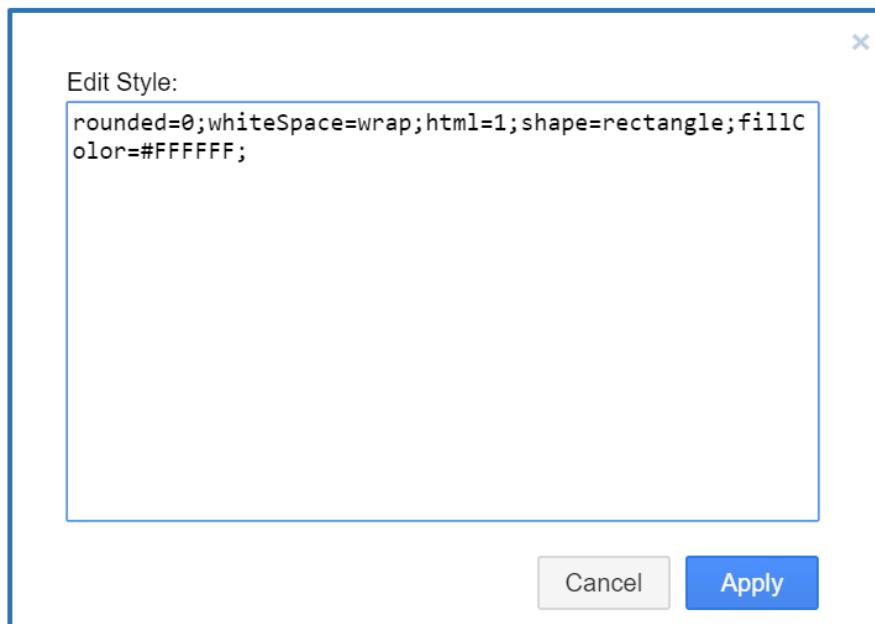


Figure: Editing a style

Edit geometry: Edit geometry allows you to edit the shape of a highlighted symbol.

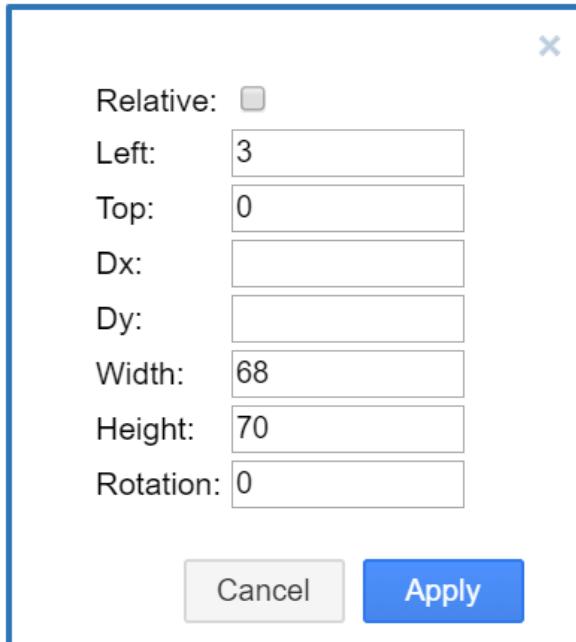


Figure: Editing shape geometry

Edit: Edit highlights a symbol's text and labels to be changed.

Edit link: Custom links can be used where hyperlinks and links to pages are allowed, namely on shapes and (parts of) text labels. To add a custom link to a cell, click on Edit Link (Alt+Shift+L) and enter it in the text box.

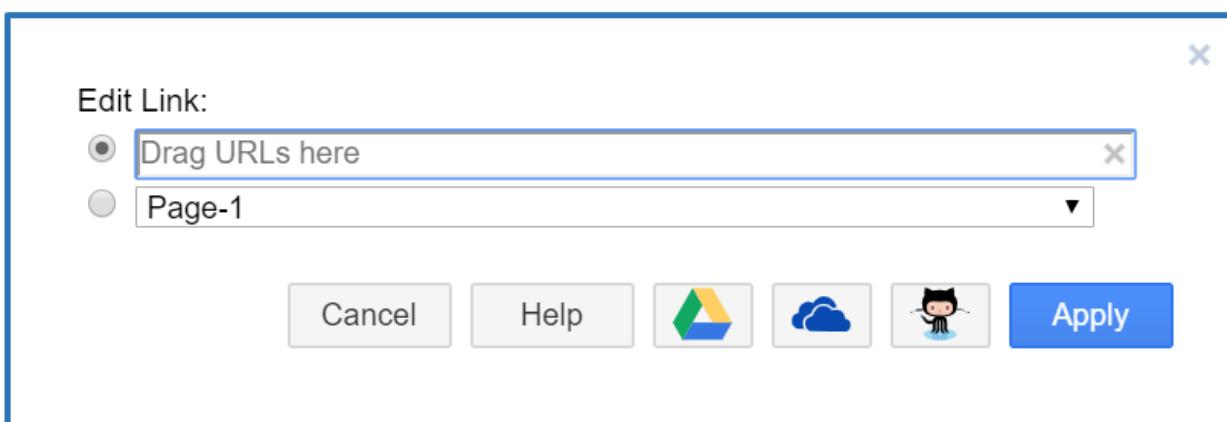


Figure: Editing a link

Advanced link customization: The format for custom links is: `data:action/json, {"actions": [actions]}` where actions is a comma-separated list of JavaScript objects (JSON) with the following possible keys:

- "open": string - opens a standard or custom link (including page links)
- "toggle"/"show"/"hide"/"highlight": cellset - toggles, shows, hides or highlights the given cells
- "select": cellset - selects the given cells if the graph is editable
- "scroll": cellset - scrolls to the first cell in the given cellset

If no scroll action is specified, then the first cell of the select or highlight action is scrolled to visible (select has precedence).

For highlight, a color (string), duration (number in milliseconds) and opacity (1-100) may be specified.

A cellset is an array of cell IDs or tags or both, e.g. `{"cells": ["id1", "id2"], "tags": ["tag1", "tag2"]}`.

To specify all cells, use "cells": ["*"], to specify all cells with a tag, use "tags": [] (empty array).

Note that if tags are used to toggle cells, the current visible state of the cell is toggled.

Example 1

```
data:action/json,{"actions":[{"toggle": {"cells": ["5", "7"]}}]}
```

Shows or hides the cells with ID 5 and 7, depending on their current visible state. Here is an example.

Example 2

```
data:action/json,{"actions":[{"open": "data:page/id,1"}, {"highlight": {"cells": ["2"], "opacity": 100, "color": "red"} } ]}
```

Opens the page with ID 1 and then highlights the cell with ID 2 in red with opacity 100%.

Example 3

```
data:action/json,{"actions":[{"show": {"tags": []}}, {"hide": {"tags": ["pipe", "water"]}}]}
```

Shows all cells with a tag and then hides all cells with tags pipe and water.

To get the ID of cells, pages and layers, use Edit Data (Ctrl/Cmd+M). To show this dialog for pages, make sure nothing is selected.

To show this dialog for layers, open the Layers window (Ctrl/Cmd+Shift+L) and click on Edit Data in the toolbar at the bottom:

If the diagram is editable, custom links are shown in a tooltip when the cell is selected and are labeled Action. When clicked, the visible state of the cells is updated, and the diagram is saved. If real-time collaboration is used, the visible state of the cells is updated in all connected diagrams. In read-only mode, clicking on the shape or text will change the visible state of the cells, but the change will not be saved.

Once a link is established you can edit it via the diagram.

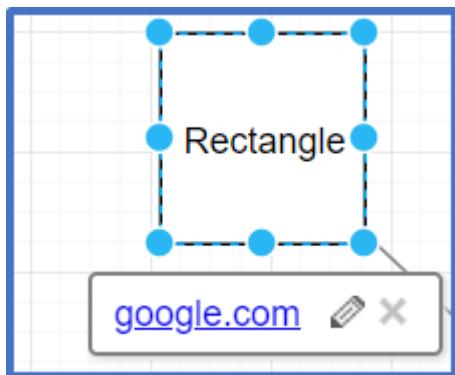


Figure: Shape with link

Open link: If there are links defined in the diagram, you can use this menu item to open the links of the symbols you have highlighted.

Select vertices: Use Select vertices to select all symbol vertices in the diagram.

Select edges: Select edges will select all the links in the diagram.

Select all: Select all will select everything defined in the diagram.

Select none: Select none will remove the highlight from all symbols/links in the diagram.

Lock/unlock: Lock will lock the symbol/link from being moved and edited. Unlock will allow those items to be editable again.

Home- View Menu

The functions under the View menu are:

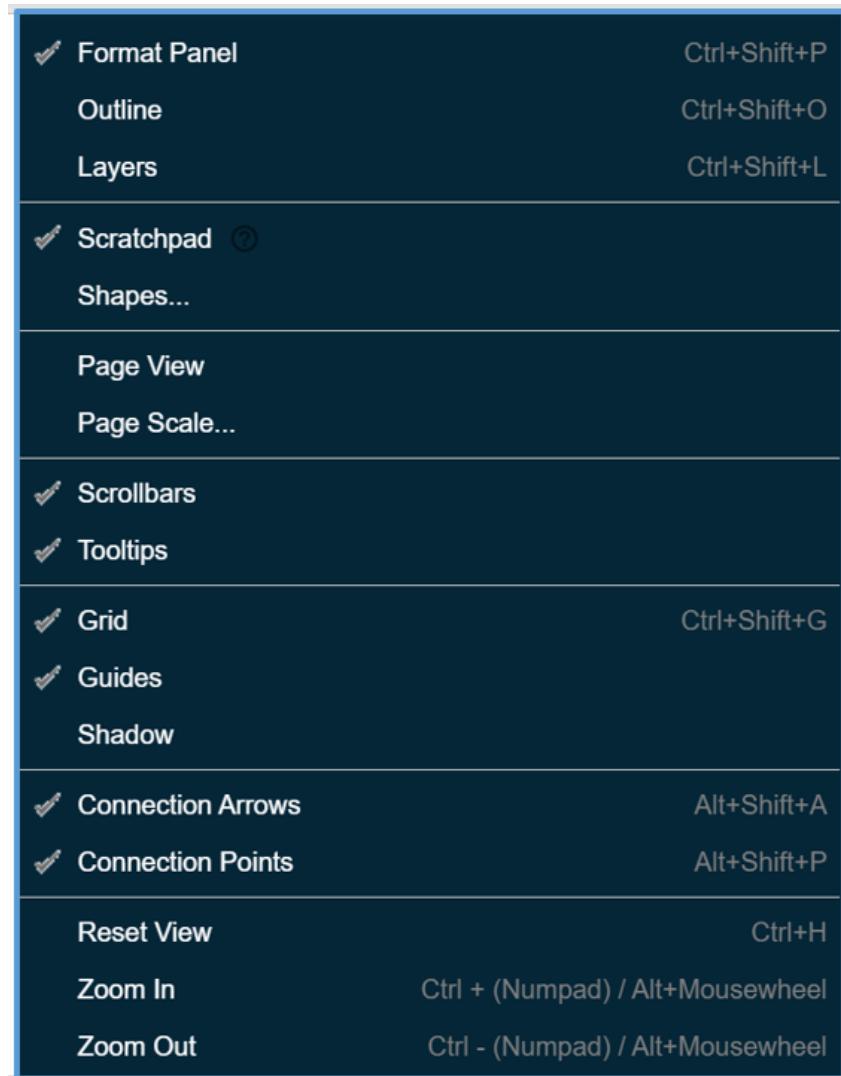


Figure: Diagram view menu

Format panel: When checked the Format panel is open on the right-side of the screen. For more about the Format panel, see the [Adding Links](#), [Adding Text](#), [Adding Symbols](#), and [Adding Zones](#) help sections. The Format Panel is unique for the different symbols in the diagram.

Outline: Outline provides a useful way of navigating through large complex diagrams. Selecting this option causes the Outline Panel to appear. Clicking and dragging the miniature page shown in the Outline Panel will also move the main page. The part of the miniature page enclosed within the blue frame corresponds to what you can see in the main page.

Similarly, you can right click and drag the main page, and watch the outline view changing as well.

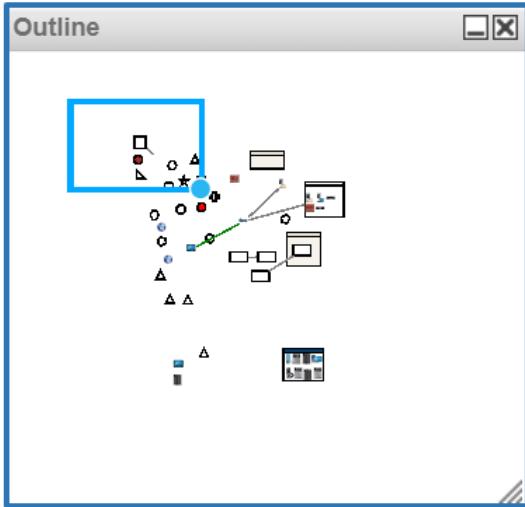


Figure: Outline panel

Layers: Layers can be useful to isolate areas visually on the diagram. Layers are often used for marking backup systems, safety systems, redundant equipment, or components in isolated physical locations such as an offsite building, fenced area, substation, or remote pumping site. However, only objects located in visible layers will be included in the compliance analysis. Symbols in invisible layers will be ignored.

When you click the Layers in the View menu, a list of available layers is shown. The Main Layer is created by default.

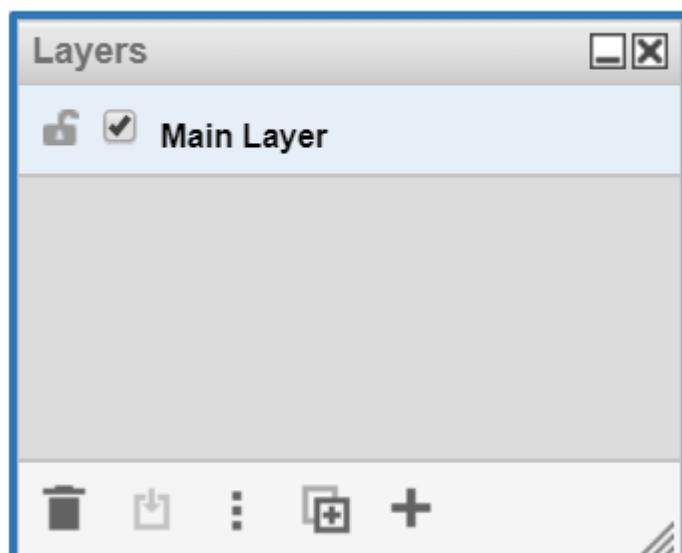


Figure: Layers popup

Add new layers

To add new layers click the plus icon at the bottom of the Layers dialogue.

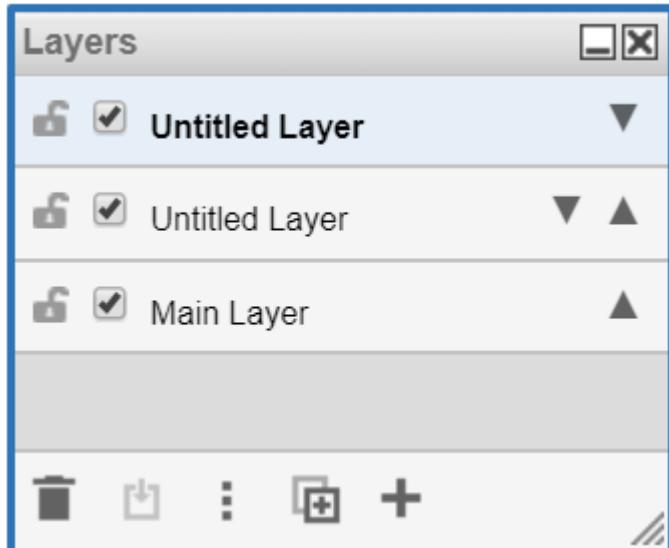


Figure: Adding new layers

All new layers are added as "Untitled Layer". Double-click to edit the layer title.

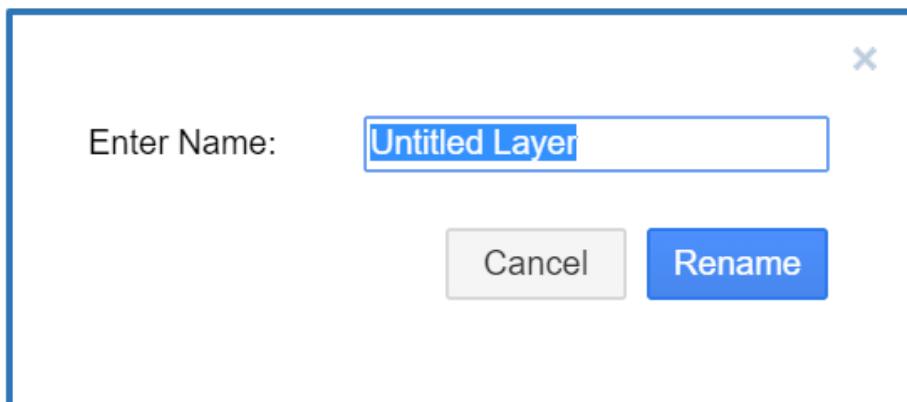


Figure: Change layer names

You can change your layers sort order by using the up and down arrows located to each individual layer in the list.

Duplicate layers

To duplicate an already existing layer, click on the layer you want to duplicate on click on the icon with two squares and a plus sign . A copy of the layer will be added to your list of layers and titled "Untitled Layer".

The Main Layer is used as a default canvas on which to place all objects. Once the component has been added, its assigned layer can be modified by selecting another layer using the Diagram Properties popup window.

Set layer visibility

To choose what layers are visible check the boxes by each individual layer.

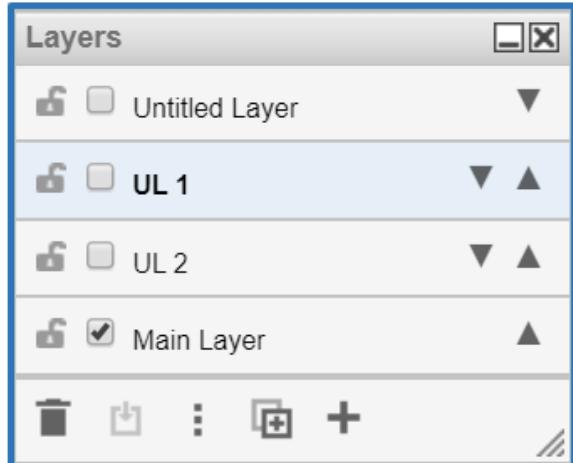


Figure: Setting layer visibility

In this window, you can set which layers are visible. Objects in invisible layers will be ignored during the analysis and in the reports.

Delete a layer

The Delete button (trash can icon) allows you to remove a layer name from the list. If you delete a layer that has components or zones assigned to it, the component assignment reverts back to the Main Layer.

Move symbols to another layer

CSET has the ability to change the layer assignment for a group of objects at one time. To make the change, simply draw the selection window around those objects that you wish to change and then select the box with an arrow icon



to see a list of the layers that you can move the items to.

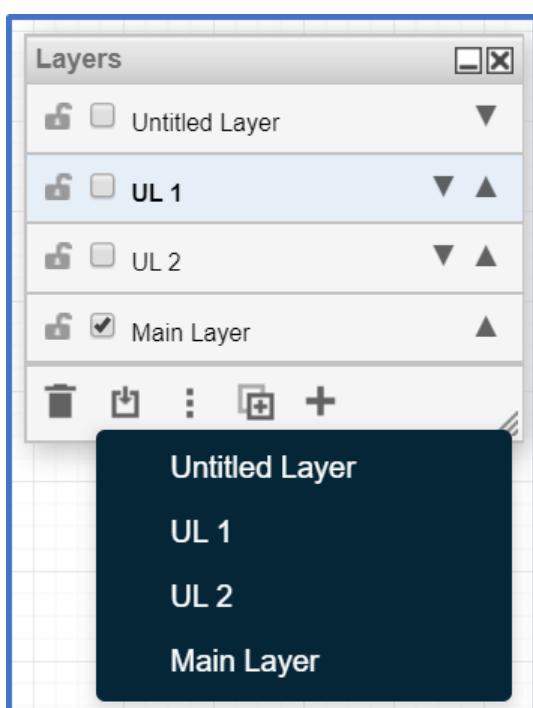


Figure: Moving a symbol to another layer

Scratchpad: The scratchpad is a temporary working space for keeping commonly used shapes for easy access. It can be found at the top left of editor, above the libraries. If it is not shown, you can display it using the menu under view > scratchpad. You can also hide it by clicking the "x" icon by the scratchpad.

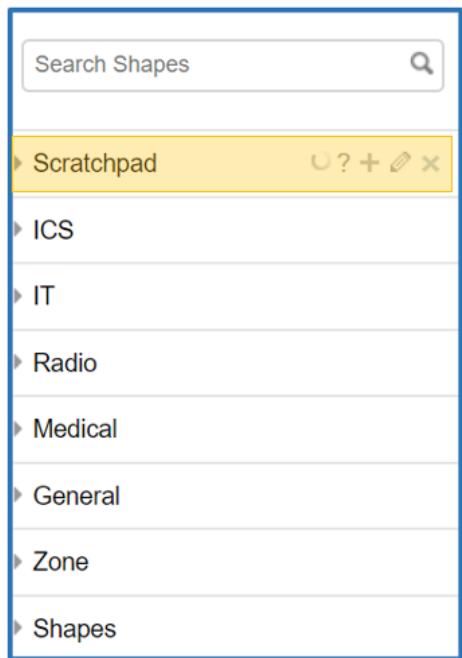


Figure: Scratchpad highlighted in the Symbols panel

To store elements in the scratchpad, drag and drop them from the diagram to the content area or click on the "+" icon while the elements are selected. To insert elements into the diagram, drag and drop them from the scratchpad to the diagram.

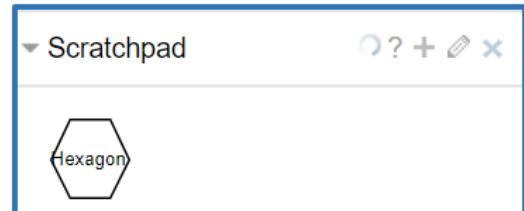


Figure: Scratchpad with saved element

To reorder or remove entries, click the pencil and use the dialog that appears. Entries can be reordered by using drag and drop. To remove entries, click on the cross icon. To add a title to an entry, click on the gray Untitled label.

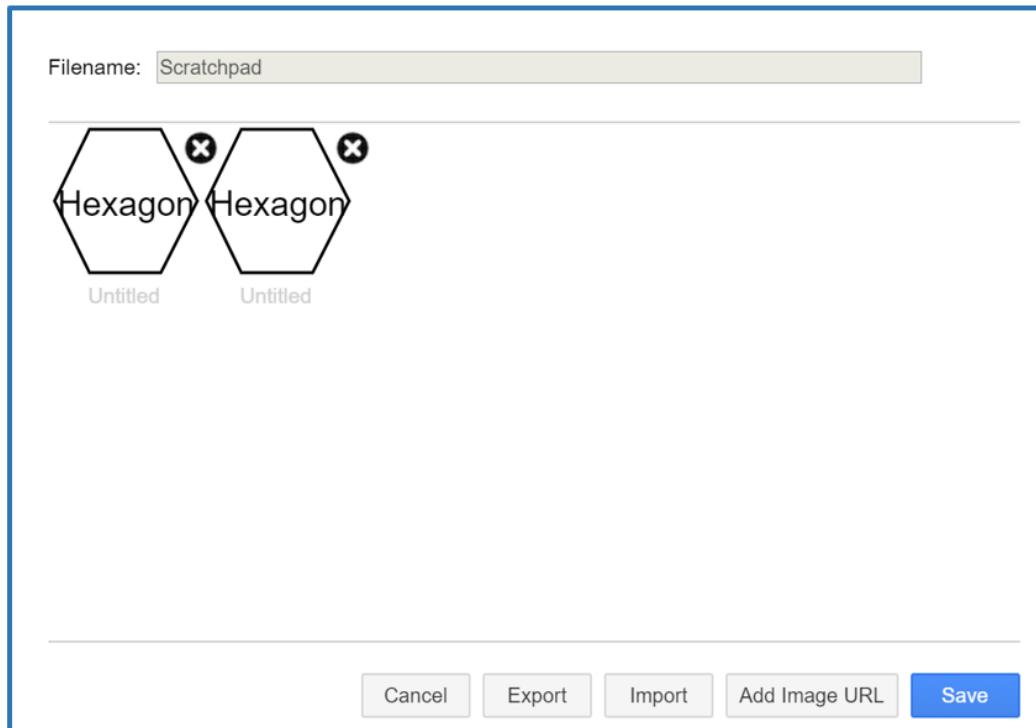


Figure: Editing scratchpad elements

Note that the scratchpad is stored in the local storage of the browser, which means its contents are deleted if cookies are cleared. The scratchpad is automatically saved between each change.

You can export the scratchpad as a .xml file from the dialog, if you want to store it more permanently or share it with others.

Shapes: Shapes allows you to customize the shapes that you want to see in the Symbols panel.

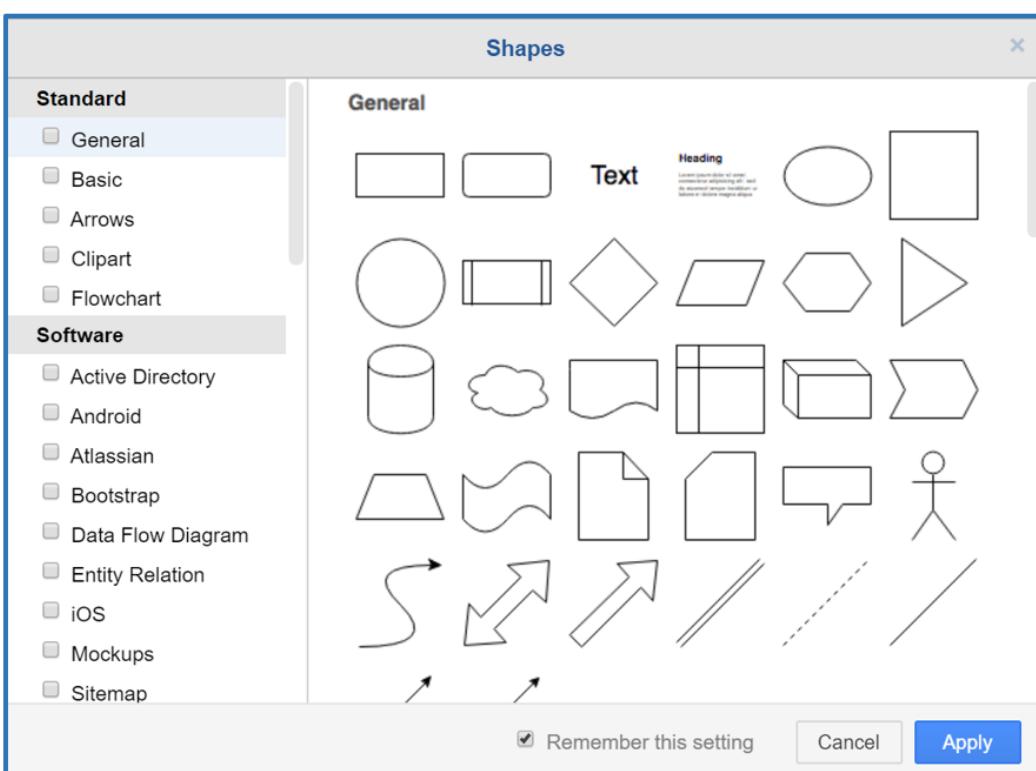


Figure: Shapes dialogue

Page view: By default, the work area appears in page view; it is sized according to the choice of paper size. Unticking this box will cause the work area to fill the entire window.

Page scale: Page scale allows you to change how the diagram fits to the page.

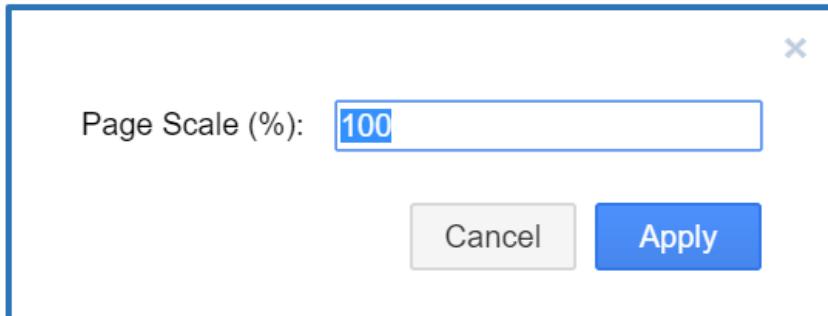


Figure: Editing the page scale

Scrollbars: This setting lets you turn on and off scrollbars.

Tooltips: This setting lets you turn on and off tooltips.

Gridlines: By default, a grid of dots is displayed on the work area, in order to help with alignment. Toggling this tick box switches the grid on and off.

Guides: By default, when moving symbols around the work area, guide lines are automatically displayed whenever a central axis or shape boundary aligns with that of another nearby shape. This is to make it easier to align shapes relative to one another. In the example below, one rectangle is being dragged by the user; its edge is currently aligned with the central axis of the other rectangle.

Toggling this tick box switches guidelines on and off.

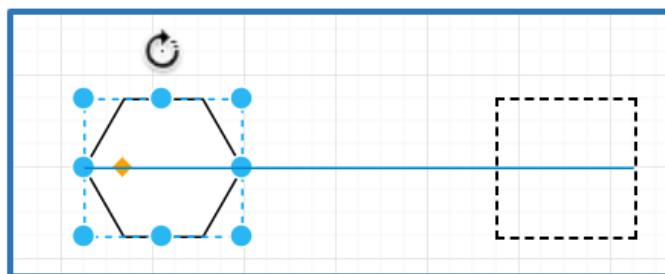


Figure: Diagram with guides on

Shadow: Selecting shadow places a shadow around the outside of the symbols.



Figure: Shape with no shadow and shape with shadow

Connection arrows: Connection arrows are the four arrows that point top, bottom, left, and right on a symbol. Clicking one of these arrows creates a copy of the symbol and a link. For more information on links, see the [Adding Links](#) help section.

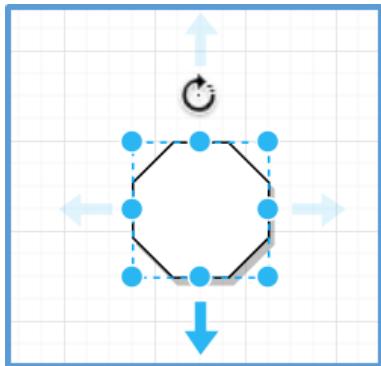


Figure: Shape with connection arrows active

Connection points: By default, hovering your mouse over a symbol will show the connection points for that symbol (see figure below), making it easier to attach a connector to the symbol. Toggling this tick box switches this feature on and off. For more information on links, see the [Adding Links](#) help section.

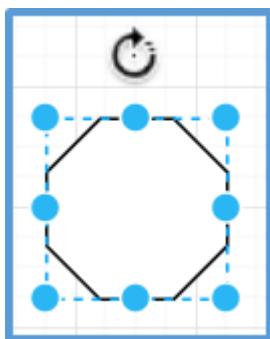


Figure: Shape with connection arrows active

Reset view: Reverses any changes to scale and maximizing or minimizing the screen.

Zoom: Zooming in or out may be done in multiple ways. Click the up or down arrows in the Zoom box to change the numeric zoom value or click inside the zoom text box and type in a zoom percentage. Zooming can also be accomplished by using the mouse wheel. The value in the Zoom box will update to match the actual zoom level.

Home- Arrange Menu

The functions under the Arrange menu are:

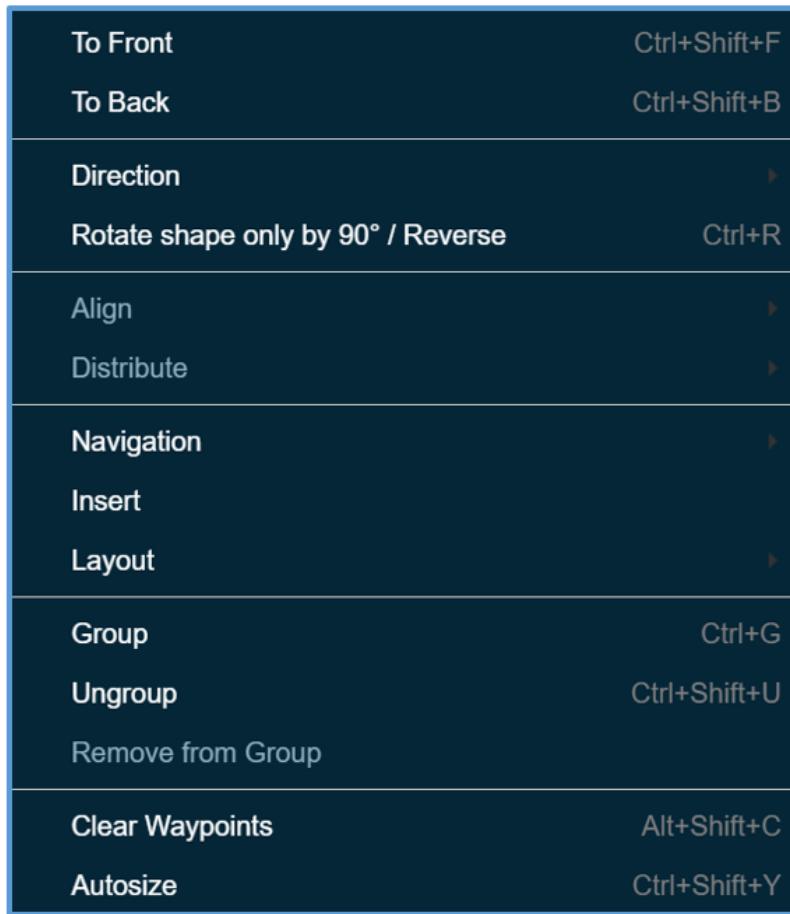


Figure: Diagram arrange menu

Bring to Front: Brings the select object to the front of all other objects.

Send to Back: Sends the selected object behind all other objects, (typically done for a zone).

Direction: Direction gives you three options to change the selected symbol: Flip horizontally, Flip vertically, and Rotation. Rotation opens a dialogue to enter a value 0-360 to rotate the symbol.

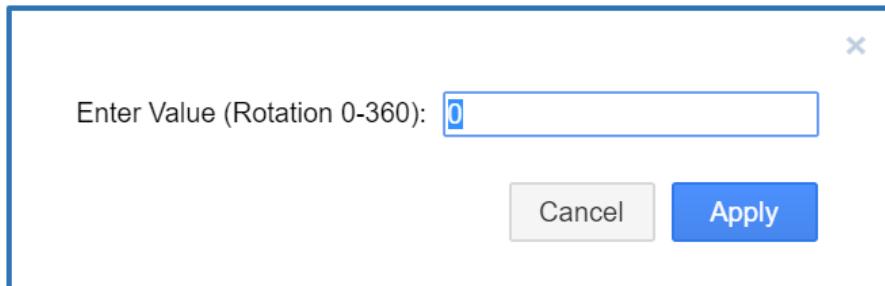


Figure: Changing shape direction

Rotate shape only by 90 degrees/reverse: This will rotate the selected symbol by 90 degrees. If you select again the action will reverse returning to how it was before rotating it.

Align

These six commands are used on groups of objects. They allow you to align objects relative to a single selected object. To use this function, select the objects to be aligned. After the objects have been selected, click on one of the buttons. The objects are moved to the respective position based on which button you clicked. Each button icon identifies what the resulting alignment will be.

Align Left: Aligns all objects to the left side of the furthest object on the left.

Align Right: Aligns all objects to the right side of the furthest object on the right.

Align Center: Aligns all objects to the center point between the furthest left and right objects selected.

Align Top: Aligns all objects to the top of the highest object selected.

Align Bottom: Aligns all objects to the bottom of the lowest object selected.

Align Middle: Aligns all objects to the center point between the highest and lowest objects selected.

Distribute: This distributes all selected symbols equally either horizontally or vertically.

Navigation: The Navigation item opens another menu:



Figure: Navigation menu

Enter group will show only the symbols that were in the defined group/zone/MSC. Clicking Exit group will return the diagram back to how it was before clicking Enter group.

Collapse will close zones/MSCs and Expand will open those back up. Collapsible will make a zone/MSC non-collapsible. Clicking Collapsible again will make the shape able to be collapsed again.

Insert:

Layout: Layout is a way to arrange symbols. A number of commonly used arrangements are available; think of them as customizable templates.

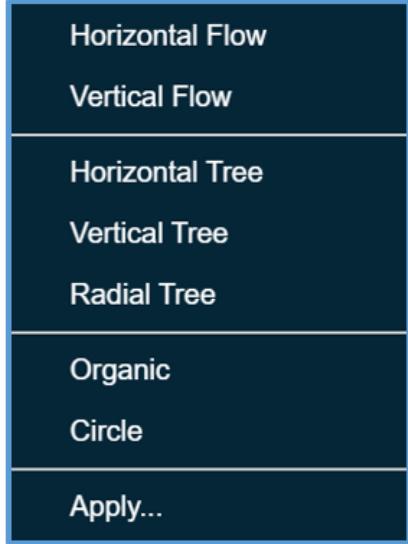


Figure: Layout menu

Flow and Tree Arrangements

Select + >Horizontal Flow as an example. When this option is selected, the arrangement screen opens.

Within this space you can start building a diagram. You are limited in the ways that we can build the diagram. Keyboard shortcuts are blocked, and there is no access to menus, panels, and toolbars. The only way to add elements is to click the > symbol on the right-hand side of a shape.

Group: Use Group to add as many symbols and links to a group as desired. Once in a group the items will all move together.

You can also use the Group (Ctrl+G/CMD+G) shortcut.

Ungroup: Use Ungroup to remove the previously grouped symbols and connectors from a group. They will each function individually now.

You can also use the Ungroup (Ctrl+Shift+U/CMD+Shift+U) shortcut.

Remove from group: Use Remove from Group to remove a specific symbol or connector out of an existing group.

Clear waypoints: Use Clear waypoints to remove all or just selected waypoints from your diagram.

Autosize: Autosize sets all selected elements to their preferred size.

Home- Extras Menu

Note: Create Shape and Edit Diagram are advanced features and are intended to be used by developers.

The functions under the Extras menu are:

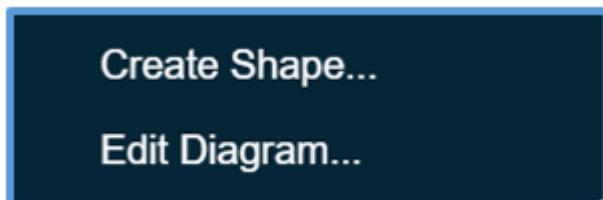


Figure: Diagram extras menu

Create shape: Shapes can be created by clicking the Create Shape button in the Extras menu. Note that there are two kinds of shapes in CSET: written in JS and in XML. The edit shape button is only shown for XML shapes (which are the less complex ones).

Here is a description of the XML format. An instructional example that tries to demonstrate a number of elements and the XSD are also available.

<shape>

The outer element is <shape>, that has attributes:

- "name", string, required. The stencil name that uniquely identifies the shape. Not used in draw.io currently.
- "w" and "h" are optional decimal view bounds. This defines your co-ordinate system for the graphics operations in the shape. The default is 100,100.
- "aspect", optional string. Either "variable", the default, or "fixed". Fixed means always render the shape with the aspect ratio defined by the ratio w/h. Variable causes the ratio to match that of the geometry of the current vertex.
- "strokewidth", optional string. Either an integer or the string "inherit". "inherit" indicates that the strokeWidth of the cell is only changed on scaling, not on resizing. If numeric values are used, the strokeWidth of the cell is changed on both scaling and resizing and the value defines the multiple that is applied to the width. Default is "1".

<connections>

If you want to define specific fixed connection points on the shape use the <connections> element. Each <constraint> element within connections defines a fixed connection point on the shape. Constraints have attributes:

- "perimeter", required. 1 or 0. 0 sets the connection point where specified by x,y. 1 Causes the position of the connection point to be extrapolated from the center of the shape, through x,y to the point of intersection with the perimeter of the shape.
- "x" and "y" are the position of the fixed point relative to the bounds of the shape. They can be automatically adjusted if perimeter=1. So, (0,0) is top left, (0.5,0.5) the center, (1,0.5) the center of the right hand edge of the bounds, etc. Values may be less than 0 or greater than 1 to be positioned outside of the shape.
- "name", optional string. A unique identifier for the port on the shape.

<background> and <foreground>

The path of the graphics drawing is split into two elements, <foreground> and <background>. The split is to define which part any shadow applied to the shape is derived from (the background). This, generally, means the background is the line tracing of the outside of the shape, but not always.

Any stroke, fill or fillstroke of a background must be the first element of the foreground element, they must not be used within <background>. If the background is empty, this is not required.

Because the background cannot have any fill or stroke, it can contain only one `<path>`, `<rect>`, `<roundrect>` or `<ellipse>` element (or none). It can also not include `<image>`, `<text>` or `<include-shape>`.

Note that the state, styling and drawing in mxGraph stencils is very close in design to that of HTML 5 canvas. Tutorials on this subject, if you're not familiar with the topic, will give a good high-level introduction to the concepts used.

State

Rendering within the foreground and background elements has the concept of state. There are two types of operations other than state save/load, styling and drawing. The styling operations change the current state, so you can save the current state with `<save/>` and pull the last saved state from the state stack using `<restore/>`.

Styling

The elements that change colors within the current state all take a hash prefixed hex color code ("#FFEA80").

- `<strokecolor>`, this sets the color that drawing paths will be rendered in when a stroke or fillstroke command is issued.
- `<fillcolor>`, this sets the color that the inside of closed paths will be rendered in when a fill or fillstroke command is issued.
- `<fontcolor>`, this sets the color that fonts are rendered in when text is drawn.

`<alpha>` defines the degree of transparency used between 1.0 for fully opaque and 0.0 for fully transparent.

`<fillalpha>` defines the degree of fill transparency used between 1.0 for fully opaque and 0.0 for fully transparent.

`<strokealpha>` defines the degree of stroke transparency used between 1.0 for fully opaque and 0.0 for fully transparent.

`<strokewidth>` defines the integer thickness of drawing elements rendered by stroking. Use `fixed="1"` to apply the value as-is, without scaling.

`<dashed>` is "1" for dashing enabled and "0" for disabled.

When `<dashed>` is enabled the current dash pattern, defined by `<dashpattern>`, is used on strokes. `dashpattern` is a sequence of space separated "on, off" lengths that define what distance to paint the stroke for, then what distance to paint nothing for, repeat... The default is "3 3". You could define a more complex pattern with "5 3 2 6", for example. Generally, it makes sense to have an even number of elements in the `dashpattern`, but that's not required.

`<linejoin>`, `<linecap>` and `<miterlimit>` are best explained by the Mozilla page on Canvas styling (about halfway down). The values are all the same except we use "flat" for `linecap`, instead of Canvas' "butt".

For font styling there are:

- `<fontsize>`, an integer,
- `<fontstyle>`, an ORed bit pattern of bold (1), italic (2) and underline (4), i.e bold underline is "5",
- `<fontfamily>`, is a string defining the typeface to be used.

Drawing

Most drawing is contained within a `<path>` element. Again, the graphic primitives are very similar to that of HTML 5 canvas.

- `<move>` to attributes required decimals (x,y).
- `<line>` to attributes required decimals (x,y).
- `<quad>` to required decimals (x2,y2) via control point required decimals (x1,y1).
- `<curve>` to required decimals (x3,y3), via control points required decimals (x1,y1) and (x2,y2).

- <arc>, this doesn't follow the HTML Canvas signatures, instead it's a copy of the SVG arc command. The SVG specification documentation gives the best description of its behaviors. The attributes are named identically, they are decimals and all required.
- <close> ends the current subpath and causes an automatic straight line to be drawn from the current point to the initial point of the current subpath.

Complex drawing

In addition to the graphics primitive operations there are non-primitive operations. These provide an easy method to draw some basic shapes:

- <rect>, attributes "x", "y", "w", "h", all required decimals
- <roundrect>, attributes "x", "y", "w", "h", all required decimals. Also "arcsize" an optional decimal attribute defining how large, the corner curves are.
- <ellipse>, attributes "x", "y", "w", "h", all required decimals.

Note that these 3 shapes and all paths must be followed by either a fill, stroke, or fillstroke.

Text

<text> elements have the following attributes:

- "str", the text string to display, required.
- "x" and "y", the decimal location (x,y) of the text element, required.
- "align", the horizontal alignment of the text element, either "left", "center" or "right". Optional, default is "left".
- "valign", the vertical alignment of the text element, either "top", "middle" or "bottom". Optional, default is "top".
- "localized", 0 or 1, if 1 then the "str" actually contains a key to use to fetch the value out of mxResources. Optional, default is 0, unused in draw.io.
- "vertical", 0 or 1, if 1 the label is rendered vertically (rotated by 90 degrees). Optional, default is 0.
- "rotation", angle in degrees (0 to 360). The angle to rotate the text by. Optional, default is 0.
- "align-shape", 0 or 1, if 0 ignore the rotation of the shape when setting the text rotation. Optional, default is 1.
- "placeholders", 0 or 1, if 1 placeholders of the form %name% will be replaced with their values. Optional, default is 0.

Images

<image> elements can either be external URLs, or data URIs, where supported (not in IE 7-). Attributes are:

- "src", required string. Either a data URI or URL.
- "x", "y", required decimals. The (x,y) position of the image.
- "w", "h", required decimals. The width and height of the image.
- "flipH" and "flipV", optional 0 or 1. Whether to flip the image along the horizontal/vertical axis. Default is 0 for both.

Sub-shapes (only supported for built-in shapes in draw.io)

<include-shape> allow stencils to be rendered within the current stencil by referencing the sub-stencil by name. Attributes are:

- "name", required string. The unique shape name of the stencil.
- "x", "y", "w", "h", required decimals. The (x,y) position of the sub-shape and its width and height.

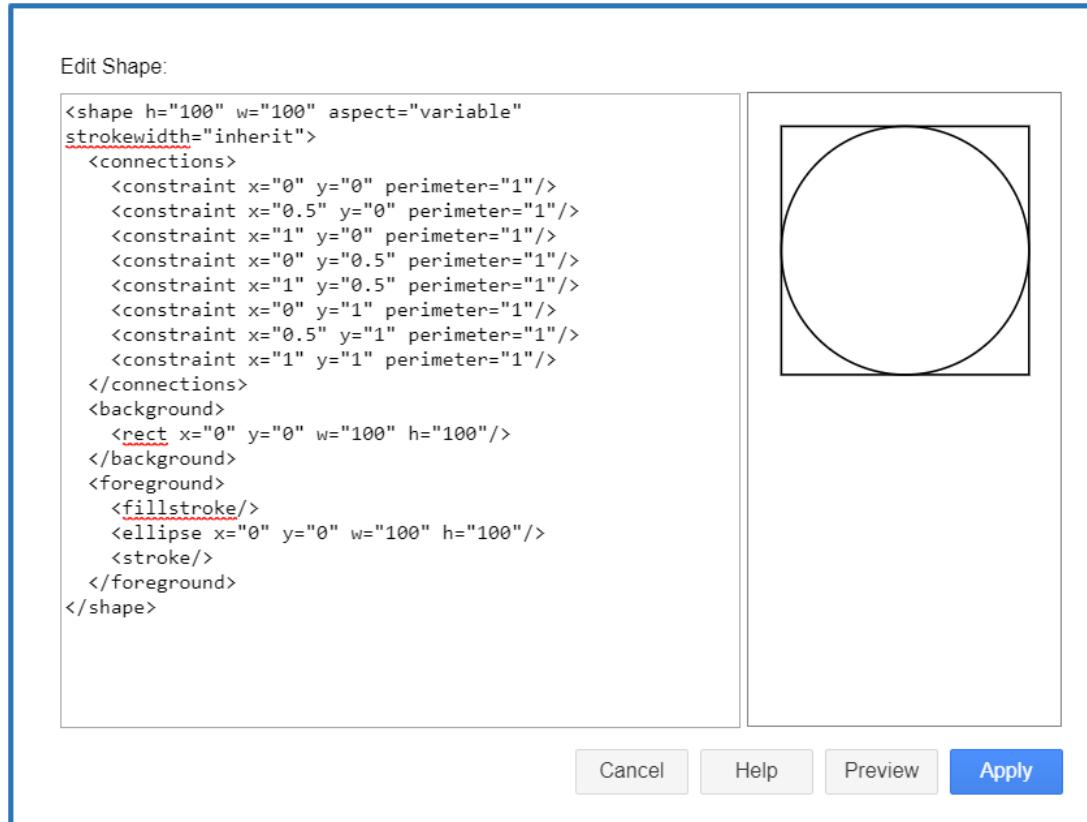


Figure: Editing shapes

Edit diagram: Selecting Edit diagram opens the mxgraph editor where you can edit the diagram.

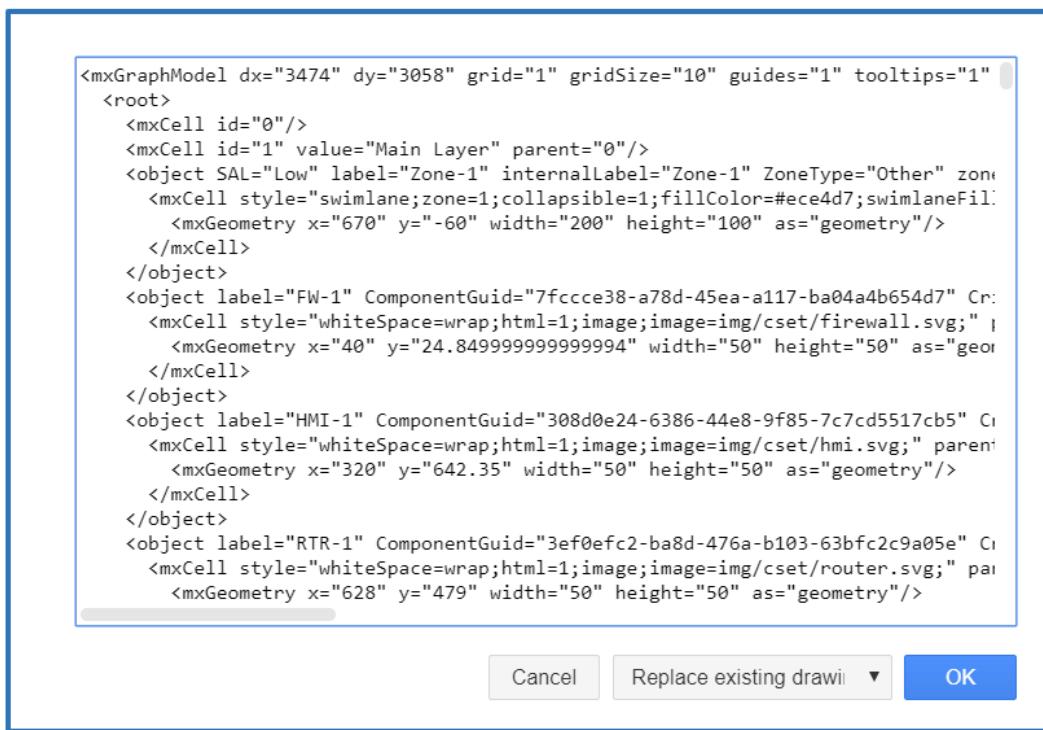


Figure: Editing the diagram

Home- Help Menu

The functions under the Help menu are:

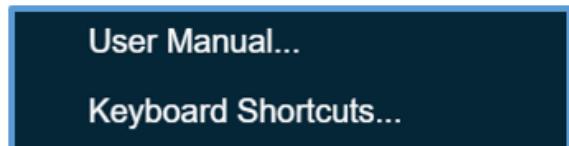


Figure: Diagram help menu

User manual: Clicking the User Manual link will open the CSET user manual bookmarked to the Diagram section help.

Keyboard shortcuts: Clicking the Keyboard shortcuts link will open a list of shortcuts that can be used in the diagram section. To see the included shortcuts, see the [Diagram Keyboard Shortcuts](#) help section.

Diagram Keyboard Shortcuts

The following keyboard shortcuts apply to the diagram. Many are similar to standard Windows shortcuts. Use the mouse to select a single item. Hold down the Control (Ctrl) keyboard key to select multiple items before applying the shortcut.

Function

Keys

Labels

Insert text or add and edge label	Double click
New line in formatted labels	Shift + Enter
New paragraph in formatted labels	Enter
Start editing label of selected cell	F2/ Enter
Stop editing and apply value	F2/ Tab/ Esc
Toggle bold/italic on selected text	Ctrl + B/I
Toggle underline on selected text	Ctrl + U
Superscript/subscript on selected text	Ctrl + ./,

Canvas

Copy	Ctrl + C
Cut	Ctrl + X
Paste	Ctrl + V
Group	Ctrl + G
Select All	Ctrl + A
Duplicate	Ctrl + D
Delete	Delete
Nudge (slightly move the selection)	Ctrl + Arrow
Nudge faster	Ctrl + Shift + Arrow
Lock/Unlock/ Edit Link	Ctrl + L/ Alt + Shift + L
Delete with Connections	Ctrl + Delete
Turn/ Rotate 90 degrees clockwise	Ctrl + R
Maintain Proportions	Shift + Resize
Centered/ Group resize	Ctrl/ Meta + Resize
Collapse Zone	Ctrl + Home
Expand Zone	Ctrl + End
Send to Back	Ctrl + Shift + B
Bring to Front	Ctrl+ Shift + F
Edit Tooltip	Ctrl + Shift + T
Autosize	Ctrl + Shift + Y
Clone Image/ Disconnect Edge	Ctrl/ Shift + Drag
Connect to a Fixed Point	Alt + Connect

Selection

Next	Tab
Previous	(Shift) + Tab
Select All/ None	Ctrl + A
Select All Vertices/ Edges	Ctrl + Shift + I/ E

Toggle Selection State Ctrl/ Shift + Click

View

Canvas Zoom in/out Alt + Mouse Wheel

Canvas Zoom in/out Ctrl + Shift + Mouse Wheel

Screen Zoom in/out Command + Mouse Wheel
(mac)

Canvas Vertical Scroll Mouse Wheel

Canvas Horizontal Scroll Shift + Mouse Wheel

Pan Canvas Space/ Right Mouse Drag

Disable Connections Ctrl + Shift + Connect

Refresh F5

Reset View Ctrl + H

Fit Window Ctrl + Shift + H

Fit Page Ctrl + J

Fit Two Pages Ctrl + Shift + J

Custom Zoom Ctrl + O

Zoom in Ctrl+ (numpad)

Zoom out Ctrl- (numpad)

Tools

Toggle Layers Window Ctrl + Shift + L

Toggle Outline Window Ctrl + Shift + O

Edit Metadata Ctrl + M

Toggle Format Panel Ctrl + Shift + P

Edit Vertex Geometry Ctrl + Shift + M

Context Menu Right Click

About F1

Sidebar/Connect

Inserts and Connects the Selected Item Alt + (Shift/ Ctrl) + Click on a
(Shift Ignores the Current Style) Sidebar Item

Replaces the Selected Item with the Shift + Click on a Sidebar
Clicked One Item

Connects the Unconnected Side of the Click on a Sidebar Item
Selected Item

Disables Connections Ctrl + Shift + Move Endpoint

Document

Save Ctrl + S

Save As Ctrl + Shift + S

Undo Ctrl + Z

Ignores Handle Under the Mouse Hold Alt

Toggle Grid Ctrl + Shift + G

Print Ctrl + P

Redo (Windows) Ctrl + Y

Redo (Linux/Mac) Ctrl + Shift + Z

Insert Text Ctrl + Shift + X

Insert Rectangle Ctrl + K

Insert Ellipse Ctrl + Shift + K

Cancel Action	Esc
Force Rubberband/ Ignore Group	Alt + Drag/Drop
Clear Default Style	Ctrl + Shift + R
Edit Style	Ctrl + E
Set as Default Style	Ctrl + Shift + D
Copy Style	Ctrl + Shift + C
Paste Style	Ctrl + Shift + V
Copy Size	Alt + Shift + X
Paste Size	Alt + Shift + V
Move Cell/ Pan Canvas	Drag
Toggle Selection/ Rubberband	Tap and Hold
Zoom	Pinch
Context Menu	Tap Selected Cell
New Line/ Apply in Safari	Ctrl/ Shift + Enter
Cancel Editing	Ctrl/ Shift + Esc
For Non-Recursive Group Resize	Ctrl + Resize
For Centered Group Resize	Ctrl + Meta + Resize

Cursor/ Page Keys

Scroll/ Move Cell (1 px)	Cursor
Move Cell (Grid Size)	Shift + Cursor
Resize Cell (1 px)	Ctrl + Cursor
Resize Cell (Grid Size)	Ctrl + Shift + Cursor
Clone and Connect	Alt + Shift + Cursor
Scroll Page	Alt + Cursor
Previous Page	Ctrl + Shift + Page Up
Next Page	Ctrl + Shift + Page Down

CMD instead of CTRL, option instead of ALT for Mac

Diagram Tool Bar

The image below shows the available options within the tool bar. Most will be familiar because they are similar to those used by popular word processing and diagramming programs. They are used to modify the format or layout of the diagram objects and text.



Figure: Diagram tool bar

View: The view dropdown allows you to customize the view of the diagram screen. There are three options: Format Panel, Outline, and Layers. You can click these options on and off to see them represented on your screen.

Zoom: Use the zoom button to change the size of the elements on the diagram screen or to use the Fit Window, Fit Page Width, Fit Page, and Two Pages functions. The magnifying glasses Zoom in and Zoom out behave very similar to the zoom percent dropdown.

Undo/Redo: Using the undo/redo buttons will either reverse your last action (undo) or reverse your last undo (redo).

Delete: Use the trash icon to delete a symbol or link. The trash icon will be grayed out unless an item is selected.

Bring Forward: Brings the selected object forward in front of any object that is one position in front of it. This is based on the relative position of one object to another so is more difficult to use.

Send Backward: Sends the select object one position behind a related object. This is based on the relative position of one object to another so is more difficult to use.

Fill: The fill button is used to fill a selected shape with color. If you select a color in the fill list, then all subsequent shapes will have that color until you select white again.

Line Color: The line color button works much the same as the fill color button. You can select from a list of colors to change the line around the highlighted shape. If you have a color selected, then all subsequent shapes will have that color outline until black is selected again.

Shadow: The shadow button will add a shadow to the symbol or link that is selected.

Connection: The connection dropdown allows you to choose the style of the link lines in your diagram.

Waypoints: The waypoint dropdown allows you to choose the style of waypoints in your diagram.



Analyze: The analyze button will turn on or off the basic network analysis. It is turned off by default and will allow the system to dynamically analyze the diagram as components, zones, or lines are either added, removed, or modified. If the button has been turned off, no analysis will take place until it has been clicked back on. For more on diagram analysis, see the [Network Deficiency](#) help section.



Fullscreen: The fullscreen button closes any side panels and makes the diagram work area the size of your screen.



Format Panel: The format panel button opens the format panel on the left-side of the screen.



Expand/Collapse: The expand/collapse button expands or collapses the top menu to show the CSET logo and assessment title.

Network Deficiency

The information related to the warnings (red dot) can be reviewed in several locations. The first and most direct way to see the message is to hover over the red dot.

In addition to the popup message that appears when you hover over the red icon, you can also review the network warnings from the Analysis screen and in the printed reports.

Each warning is identified by a numbered red circle in proximity to the line or component to which it refers.

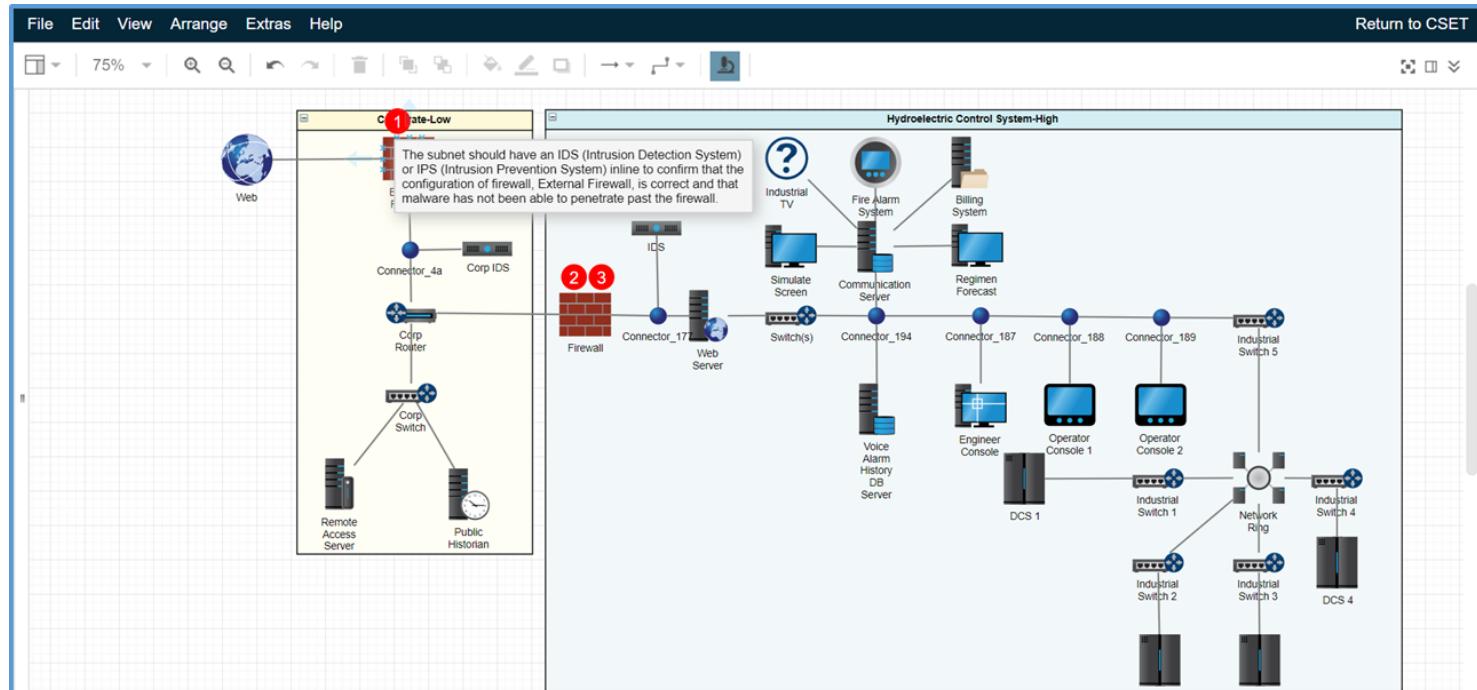


Figure: Diagram screen with network analysis work

Network Analysis Rules

This section of the user guide describes the network analysis rules found in the network diagram editor. It may be worthwhile to review these rules as guidelines for a basic network architecture.

Rule 1: There must be a firewall or other border protection devices (data diode) between different network enclaves (zones).

"The network path identified by the components, {0} and {1}, appears to connect network segments whose components reside in different zones. A firewall to filter the traffic on this path is recommended to protect the components in one zone from a compromised component in the other zone.";

Additional Description: The purpose of a network enclave is to limit internal access to a portion of a network. It's necessary when the set of resources differs from those of the general network surroundings. Typically, network enclaves are not publicly accessible. Internal accessibility is restricted through the use of internal firewalls, VLANs, network access control, and VPNs.

Segmenting a network into separate enclaves prevents either an internal or external threat attacker from moving freely through the network. Organizations that implement a secure network design will find that the added cost and complexity of segmentation is more than offset by a reduction in number and severity of incidents. The effort extended in learning, classifying, and segmenting the network helps your network administrators and architects to better understand the network, both from a performance and security perspective. This adds value and strengthens all of the organization's controls.

Rule 2: Firewalls should have an associated IPS or IDS to monitor traffic and confirm firewall configuration.

The subnet, "Subnet Name", should have an IDS (Intrusion Detection System) or IPS (Intrusion Prevention System) inline to confirm that the configuration of firewall, "Firewall Name", is correct and that malware has not been able to penetrate past the firewall.

Additional Description: There are two common types of IDS systems: Host based and Network based. Host Intrusion Detection Systems(HIDS) are installed on the host and watch network traffic and system information for indicators of intrusion. Network Intrusion Detection Systems (NIDS) only monitor network traffic. This rule refers to NIDS. Intrusion Prevention Systems (IPS) are based on the same principles and techniques as an IDS but adds the additional functionality of responding to network intrusions

Rule 3: Separating enclaves (zones) strictly by VLANs does not necessarily protect traffic between VLANs.

"The separate subnets handled by the VLAN component, {0}, carry traffic of different SALs. The incorrect configuration of the component, or the possible compromise of the component, allow the critical traffic to be visible on the less protected network segment.";

Additional Description: See the following article for additional discussion. https://www.nsa.gov/Portals/70/documents/resources/everyone/csfc/capability-packages/MSCCPv1.1_20180626.pdf

Rule 4: No multi-homed devices. Multiple interfaces in a component may act as a bridge between the different enclaves.

"The component, {0}, has multiple interfaces where the subnets of those interfaces carry traffic of different SALs. If the component is compromised, the critical traffic could be visible from the less protected network.";

Additional Description: This bridges networks by allowing multi-homed devices to bypass your security controls and allows an attacker to freely pivot from one network to another. A multi-homed device is any device with multiple network cards or interfaces.

Rule 5: No backdoor modems or unprotected third-party connections

"The path identified by the components, {0} and {1}, appears to connect on one side to an external network. A firewall to filter the traffic to and from the external network is recommended to protect the facility's network. Note that a 'Web' component, 'Vendor' component, or 'Partner' component are all assumed to interface with an external network. In addition, a modem with a single connection is assumed to allow a connection from outside the facility's network.";

Additional Description: A backdoor connection is a modem or other connection that bypasses all the regular security checks when accessing the system through the regularly recognized means. Attackers find and use these connections to access your system. These backdoor connections should either be eliminated or require the same level of security access and control as any other external connection.

Rule 6: No open untrusted links. Either firewall it off or wrap in VPN or Encrypted Tunnel.

"The path between the components, {0} and {1}, is untrusted. Because malicious traffic may be introduced onto the link, a firewall to filter the traffic on both sides of untrusted link is recommended.";

Additional Description: An untrusted link is any link that may have potential public access. This can be a line that has open physical access, or it can be a connection that crosses the internet unencrypted. Attackers can use this open access to see the data in the connection or change the information to compromise your system.

Rule 7: Correct Data Flow on Unidirectional devices.

"Data flow between two distinct SAL zones via a unidirectional {0} must only flow from a higher SAL to a lower SAL. Example Control or SCADA network SAL High to Corporate Network SAL Low, but not SAL Low to SAL High.";

"Data flow between two distinct SAL zones via a unidirectional {0} must only flow from a lower SAL to a higher SAL. Example unclassified network to classified network";

Additional Description: This one is a little bit more nuanced. When working in a control system or SCADA environment data should be able to flow out of the environment but not in (i.e. availability is important, but confidentiality is unimportant). When working in a data protection environment (e.g. classified) data may flow into the environment but not out.

A **unidirectional network** (also referred to as a **unidirectional gateway** or **data diode**) is a network appliance or device that allows data to travel in only one direction. Data diodes can be found most commonly in high security environments, such as defense, where they serve as connections between two or more networks of differing security classifications. Given the rise of industrial [IoT](#) and [digitization](#), this technology can now be found at the industrial control level for such facilities as [nuclear power plants](#), [power generation](#) and [safety critical systems](#) like railway networks.

After years of development the use of data diodes has increased creating two variations:

- [**Data diode**](#): Network appliance or device allowing raw data to travel only in one direction, used in guaranteeing information security or protection of critical digital systems, such as industrial control systems, from inbound cyber attacks.
- [**Unidirectional gateway**](#): Combination of hardware and software running in proxy computers in the source and destination networks. The hardware, a data diode, enforces physical unidirectionality and the software replicates databases and emulates protocol servers to handle bi-directional communication. The unidirectional gateway is capable of transferring multiple protocols and data types simultaneously. It contains a broader range of [cybersecurity](#) features like, [secure boot](#), [certificate management](#), [data integrity](#), [forward error correction](#) (FEC), secure communication via [TLS](#), among others. A unique characteristic is that data is transferred deterministically (to predetermined locations) with a protocol "break" that allows the data to be transferred through the data diode.

Data diodes are commonly found in high security military and government environments, and are now becoming widely spread in sectors like [oil & gas](#), water/wastewater, [airplanes](#) (between flight control units and in-flight

entertainment systems), [manufacturing](#) and [cloud](#) connectivity for [industrial IoT](#). New regulations have increased demand and with increased capacity, major technology vendors have lowered the cost of the core technology.

Assessment Section

The assessment section is where the user answers questions related to the selected Standards or Profile and Security Assurance Level. The following sections will describe the Assessment process in detail.

Assessment Screen

The primary interaction that takes place in CSET happens on the Assessment screen. The Assessment screen displays sets of questions or requirements for the user to read and answer based on the selected assessment mode, the actual Standards chosen, the security assurance level (SAL), and the components used on the diagram tool. The results of the combined answers to the presented questions will help to provide a good perspective and understanding of the organization's cybersecurity posture.

Completing the questions portion of the assessment is where most of the time will be spent. The process of answering questions is not difficult but it can be tedious. It is recommended that the user plan ahead and recognize that it will take several hours or even days to accurately answer all the questions. The more time spent understanding the intent of each question and then discussing it as a team, the more valuable will be the assessment. Take the time to fully understand the intent of each question then provide the answer that best meets the current situation. If upgrades are in progress at the time of the assessment, comments can be associated with the relevant questions to document the activity.

The Assessment screen will display different content based on the selected assessment mode. For more information about the different content displayed based on the assessment mode, see the [Assessment Modes](#) help section.

The figure below shows the main sections of the Assessment screen.

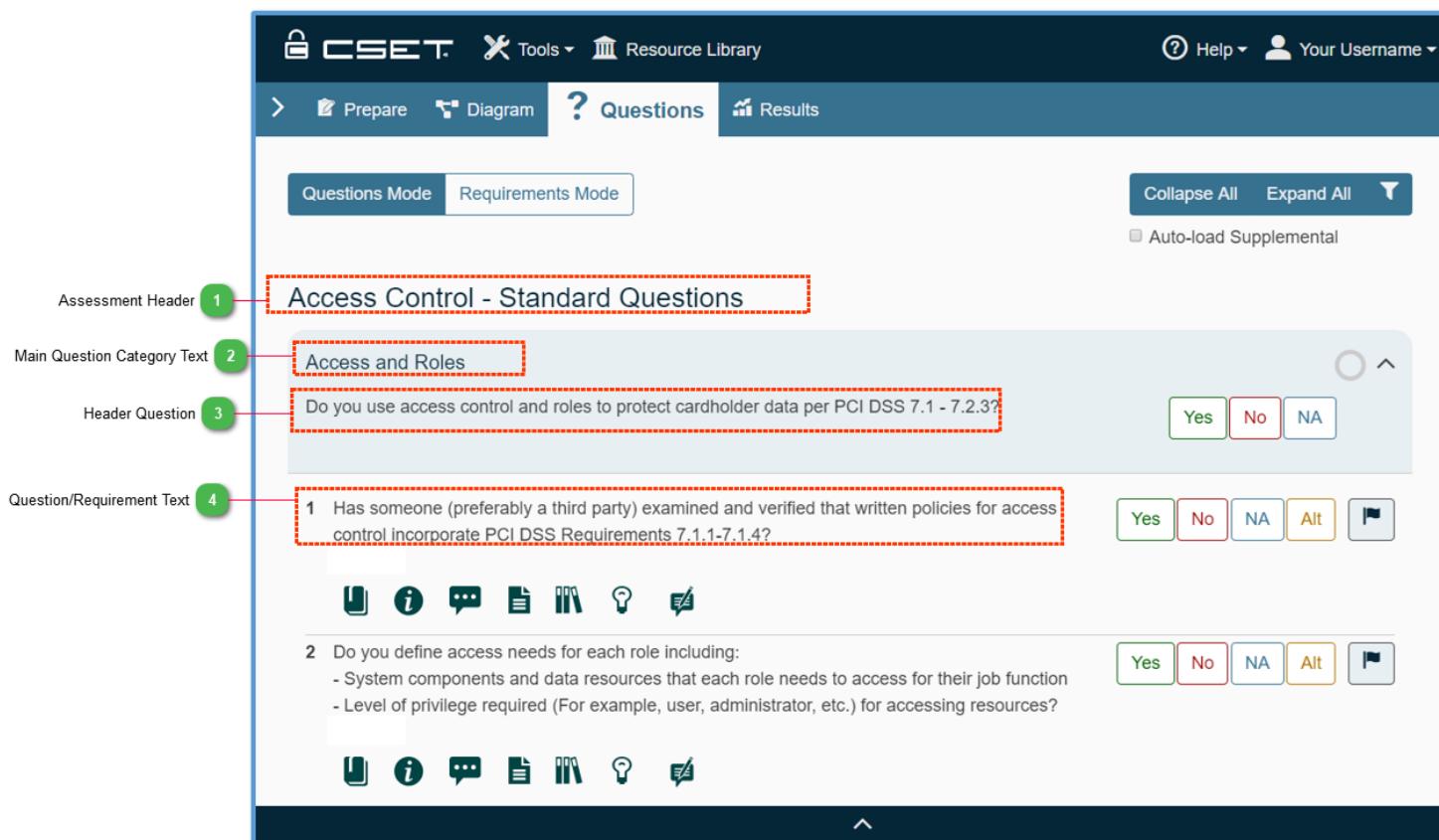


Figure: Assessment screen

1

Assessment Header

Access Control - Standard Questions

The assessment header contains controls for managing the questions displayed in the Question/Requirement Text section.

2 Main Question Category Text

Access and Roles

The green Main Question Category Text displays the high-level categories in which groups of questions or requirements belong.

3 Header Question

Do you use access control and roles to protect cardholder data per PCI DSS 7.1 - 7.2.3?

For Header Questions (only seen in the Questions mode) if the user answers "No" all the following questions in the category will be marked "No." Answering "Yes" or "NA" doesn't have the same behavior.

4 Question/Requirement Text

- 1 Has someone (preferably a third party) examined and verified that written policies for access control incorporate PCI DSS Requirements 7.1.1-7.1.4?

The Question/Requirement Text contains the questions and requirements of the assessment as well as the answers and supplemental information.

The answers for all questions will be Yes, No, Not Applicable, and Alternative Response. The process is simple. Read the question in detail and then answer yes if the question language and intent are met, or no if the question language and intent are not met. The colors of the answers reflect the answer given. The colors provide a quick visual reference of how the user is doing in each category.

Yes answers are green, No answers are red, Not Applicable answers are blue, and ALT answers are light green.

In addition to clicking the answers with the mouse, shortcut keys are available to use with this screen. The full list of keyboard shortcuts is available in the help section titled [Keyboard Shortcuts](#).

The Not Applicable is used when the question does not apply to the system or facility. It should be used with discretion and has the effect of removing the question from consideration. Any questions marked as Not Applicable will not show up in the online analysis or reports as a gap or missed answer; nor will they count as a positive answer.

The ALT label stands for Alternate and is used when an alternate or different method is being used to address the concern in the question. For example, a question may be asked about whether the servers are located behind locked doors with certain access restrictions. The facility may not have locked doors, but instead, employ a security guard at the door to the server room. This different (security guard) approach does not directly answer the question, but the user may feel like this alternate approach to securing the room is either equal to or better than locks on the doors. An alternate method is scored in a positive way similar to a Yes answer.

If an alternate method is selected, then the user should fill in the description in the Question Details panel in the text box under the label Alternate Description/Justification. The Question Details panel is opened when the Details tab is clicked.

Assessment Modes

The questions on the assessment screen will change based on the assessment mode selected. Questions are organized into categories and different information is displayed based on the selected mode. There are three modes of operation that affect the display of questions:

1. Questions Mode,
2. Requirements Mode

Questions Mode

The Assessment Screen in Questions mode displays simple to read questions on the Assessment screen. Next to the questions is Supplemental Information from the associated requirement in the related Standard.

The unique characteristics of the Assessment Screen in Questions mode are shown on the [Assessment Screen Questions Mode](#) page.

Requirements Mode

The Assessment Screen in Requirements mode displays the exact wording of the requirement text in the associated Standard.

The unique characteristics of the Assessment Screen in Requirements mode are shown on the [Assessment Screen Requirements Mode](#) page.

Assessment Screen Questions Mode

The figure below displays the Assessment screen in Questions mode. Questions mode is the recommended assessment mode for most users.

The screenshot shows the CSET software interface in Questions mode. The top navigation bar includes 'CSET', 'Tools', 'Resource Library', 'Help', and 'Your Username'. Below the bar, tabs for 'Prepare', 'Diagram', 'Questions' (which is selected), and 'Results' are visible. A secondary navigation bar at the top of the main content area has 'Questions Mode' (selected) and 'Requirements Mode' buttons, along with 'Collapse All', 'Expand All', and a search icon. A checkbox for 'Auto-load Supplemental' is also present. The main content area is titled 'Access Control - Standard Questions' and contains a section titled 'Access and Roles' with the question 'Do you use access control and roles to protect cardholder data per PCI DSS 7.1 - 7.2.3?'. Below this is a list of requirements:

- 1 Has someone (preferably a third party) examined and verified that written policies for access control incorporate PCI DSS Requirements 7.1.1-7.1.4?
- 2 Do you define access needs for each role including:
 - System components and data resources that each role needs to access for their job function
 - Level of privilege required (For example, user, administrator, etc.) for accessing resources?

Each requirement has a set of response buttons ('Yes', 'No', 'NA', 'Alt') and a flag icon. Below the requirements is a row of icons: a clipboard, a magnifying glass, a speech bubble, a document, a barcode, a lightbulb, and a gear.

Figure: Assessment screen in questions mode

Questions mode toggle: The Questions Mode button is blue when selected. This indicates that the user is in the Questions Mode screen.

Questions mode- Question text: Questions Mode questions have been prepared using straightforward language. The questions encompass all the topics and requirements found in the major ICS and IT Standards. The questions are generally fairly short compared to their associated requirements from the underlying Standard. The question text is typically a subset of the underlying requirement text.

Assessment Screen Requirements Mode

The figure below displays the Assessment screen in Requirements mode. Requirements mode is recommended for regulated industries where the exact wording of the Standard is important.

The screenshot shows the CSET Assessment interface in Requirements mode. The top navigation bar includes 'CSET', 'Tools', 'Resource Library', 'Help', and 'Your Username'. Below the bar, tabs for 'Prepare', 'Diagram', 'Requirements' (selected), and 'Results' are visible. A mode toggle at the top left shows 'Requirements Mode' is active. On the right, buttons for 'Collapse All' and 'Expand All' are present, along with a checkbox for 'Auto-load Supplemental'. The main content area is titled 'Build and Maintain a Secure Network and Systems - PCI DSS'. It displays a requirement: 'Install and maintain a firewall configuration to protect cardholder data'. Below this is a detailed test description: 'Test 1.1 1.1 Inspect the firewall and router configuration standards and other documentation specified below and verify that standards are complete and implemented as follows:'. This is followed by a list of icons: Uncheckable, Information, Comment, Document, Network, Idea, and Note. Three specific requirements are listed with their own descriptions and status buttons (Yes, No, NA, Alt, Flag):

- Req 1.1.3** 1.1.3 Current Diagram That Shows All Cardholder Data Flows Across Systems And Networks. Icons: Uncheckable, Information, Comment, Document, Network, Idea, Note.
- Req 1.1.1** 1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations. Icons: Uncheckable, Information, Comment, Document, Network, Idea, Note.

Figure: Assessment screen in requirements mode

Requirements mode toggle: The Requirements Mode button is blue when selected. This indicates that the user is in the Requirements Mode screen.

Requirement Identifier: Requirements mode displays the Requirement Identifier instead of a question number.

Requirement text: Requirement Text displays requirements directly from the standard for users to answer.

Assessment Categories

Question sets are divided into categories depending on the assessment mode, Standards, and SAL selected. Different categories are displayed in multiple areas on the Questions screen based on the Assessment mode such as the bread crumb navigation control, the titles above the questions, and In the Question Details Section.

The figure below shows some examples of Question Categories in Questions mode.

The screenshot shows the CSET software interface in 'Questions Mode'. The top navigation bar includes 'CSET', 'Tools', 'Resource Library', 'Help', and 'Your Username'. Below the navigation is a breadcrumb menu with 'Prepare', 'Diagram', 'Questions' (which is highlighted), and 'Results'. A toolbar at the top right includes 'Collapse All', 'Expand All', and a search icon. The main content area displays a list of questions under 'Access Control - Standard Questions' (highlighted with a red dashed box). The first question is: 'Does the registration process require authenticators to be given in person by authorized personnel?'. To the right of the question are five response buttons: 'Yes' (green), 'No' (red), 'NA' (blue), 'Alt' (yellow), and a flag icon. Below the question are icons for edit, info, comments, file, and help. Detailed information for the question includes: Title: PR.AC-1, Category: Access Control, Security Assurance Level (SAL): Low, and Standard Specific Requirement: 'Identities and credentials are managed for authorized devices and users.' (also highlighted with a red dashed box). At the bottom of the screen, there is a 'Least Privilege' footer.

Figure: Question Categories

1 Main Category text

Access Control - Standard Questions

All questions in CSET have been grouped into main categories. The main categories are high level groupings for questions and are used as high level groupings for improved navigation and in the assessment results.

2 Sub Category text

Authenticator Management

The Standard Specific text is the category associated with the question in the requirement text of the associated Standard. The Standard Requirement Category can be found in associated reference documentation related to each question.

3 Standard Specific text

Standard Specific Requirement:

Identities and credentials are managed for authorized devices and users

The Standard Specific text is the category associated with the question in the requirement text of the associated Standard. The Standard Requirement Category can be found in associated reference documentation related to each question.

Question Details, Resources, and Comments

The Question Details, Resources, and Comments contains extra detailed information about the currently selected question. The user can also add comments, discoveries, and reference documents to the question or requirement as well as mark the question or requirement for further review. The figure below describes the Question Details, Resources and Comments screen.

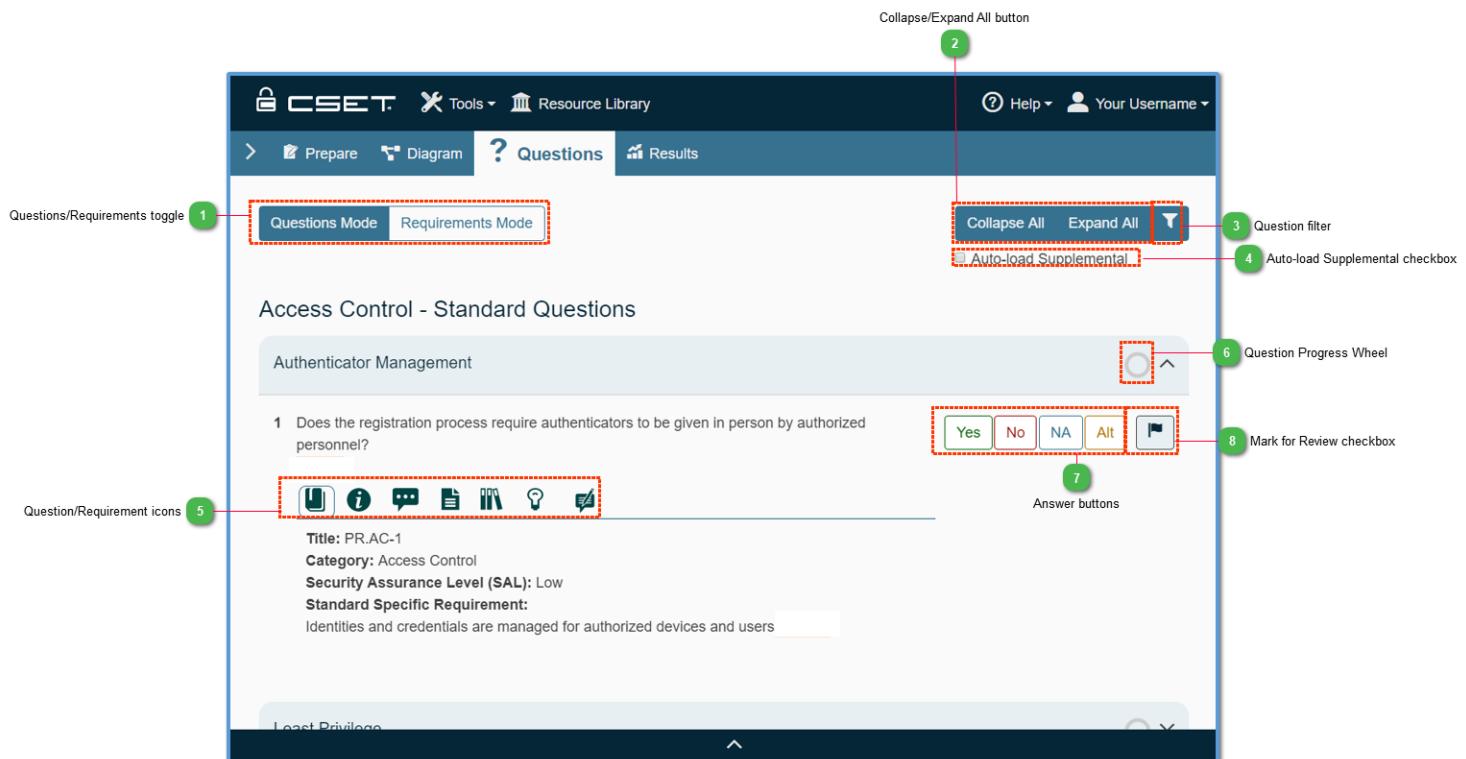


Figure: Question Details, Resources, and Comments Screen

1 Questions/Requirements toggle



The Question/Requirements toggle allows a user to switch between Question and Requirements mode.

2 Collapse/Expand All button



Click the Collapse All button to close all question categories, and the Expand All button to open all question categories.

3 Question filter



Clicking the Question filter allows the user to filter the assessment questions by answer, whether an assessment has comments, discoveries, or has been marked for review.

4 Auto-load Supplemental checkbox

Auto-load Supplemental

Clicking the Auto-load Supplemental checkbox will automatically load supplemental information as the user scrolls through questions.

5 Question/Requirement icons



The Question/Requirement icons are described in detail below.

Supplemental button : Clicking the Supplemental button opens up the supplemental information for the questions.

See the [Supplemental Section](#) for more information.

Comments button : Clicking the Comments button opens the Comments Section of the Details and Resources panel allowing the user to enter comments related to the current question or requirement.

See the [Comments Section](#) for more information.

Documents button : Clicking the Documents button opens the Documents section of the Details and Resources panel allowing the user to associate related documents to the question or requirement.

See the [Documents Section](#) for more information.

References button : Clicking the References button opens the References section of the Details and Resources panel allowing the user to open Standards that are associated with and referenced in the assessment question.

See the [References Section](#) for more information.

Observations button : Clicking the Observations button opens the Observations section of the Details and Resources panel allowing the user to create a discovery record to associate to the question or requirement.

See the [Observations Section](#) for more information.

Feedback button : Clicking the Feedback button opens the Feedback section of the Details and Resources panel allowing the user to leave feedback for DHS or FAA.

See the [Feedback Section](#) for more information.

6 Question Progress Wheel



The Question Progress Wheel indicates how many questions a user has filled out. The checkmark means that all questions in the category have been answered.

7 Answer buttons



Click "Yes", "No", "NA", or "Alt" to answer questions.

8 Mark for Review checkbox



The Mark for Review checkbox allows the user to mark a question or requirement for future review.

Details Section Question Mode

The Question or Requirements Details section will contain different controls and text depending on the selected assessment mode. The figure below describes the Details section in Question Mode.

Figure: Details section question mode

1 Title text

Title: PR.AC-1

The Title text is a textual identifier for the question usually related to the Standard to which it belongs.

2 Category text

Category: Access Control

The Category text is the Standard category of the question. Questions typically reside in multiple categories. The Category text here indicates the category in the related Standard to which that the question belongs.

For more information about question categories, see the [Assessment Categories](#) help section.

3 Security Assurance Level text

Security Assurance Level (SAL): Low

The Security Assurance Level text is the highest SAL of the question. All questions and requirements have SAL value assigned to them. The Security Assurance Level text indicates the SAL for the question. When users select a SAL and a Standard during the preparation process, they will get all questions in their selected Standard that have the same or lower SAL they selected. For example, if users selected a High SAL and the Key Standard, they will get all questions in Key that are High, Medium, and Low.

Standard Specific Requirement text

Standard Specific Requirement:

Identities and credentials are managed for authorized devices and users

The Standard Specific Requirement text is the requirement text from the Standard associated with the question. If the user is in the Requirements assessment mode, the Standard Specific Requirement text will be the same as the question text. Note: There are also many instances where Standard Specific Requirement text will be the same as the question text.

Details Section Requirements Mode

The Question or Requirements Details section will contain different controls and text depending on the selected assessment mode. The figure below describes the Details section in Requirements Mode.

The screenshot shows the CSET application interface in Requirements Mode. The top navigation bar includes links for Tools, Resource Library, Help, and Your Username. Below the navigation is a toolbar with Prepare, Diagram, Requirements (selected), and Results. A secondary toolbar at the top of the main content area includes Questions Mode, Requirements Mode, Collapse All, Expand All, and Auto-load Supplemental. The main content area displays a requirement titled "Identify - Cybersecurity Framework" under the "Asset Management" category. Requirement ID.AM-1 is listed: "Physical devices and systems within the organization are inventoried". To the right of the requirement are four status buttons: Yes (green), No (red), NA (blue), and Alt (orange). Below these buttons are five small icons: a document, a magnifying glass, a speech bubble, a file, and a key. The requirement details section includes fields for Title (ID.AM-1), Category (Asset Management), Security Assurance Level (SAL), and Questions Related to this Requirement. The "Questions Related to this Requirement" section lists two bullet points:

- Has an inventory list of the components of the system been developed, documented, and maintained that is consistent with the system boundary?
- Has an inventory list of the components of the system been developed, documented, and maintained that is at the level of granularity deemed necessary for tracking and reporting?

Figure: Details section requirement mode

Questions Related to this Requirement: The main difference between the Question and Requirements modes is that Requirements Mode has the extra Questions Related to this Requirement text. The Questions Related to this Requirement text displays all questions identified by the Requirement.

Supplemental Section

Questions and Requirements on the Assessment screen will almost always have supplemental information. The figure below describes the assessment screen focusing on Supplemental information.

ID.AM-1 Physical devices and systems within the organization are inventoried

Organizations may choose to implement centralized information system component inventories that include components from all organizational information systems. In such situations, organizations ensure that the resulting inventories include system-specific information required for proper component accountability (e.g., information system association, information system owner). Information deemed necessary for effective accountability of information system components includes, for example, hardware inventory specifications, software license information, software version numbers, component owners, and for networked components or devices, machine names and network addresses. Inventory specifications include, for example, manufacturer, device type, model, serial number, and physical location.

Figure: Question supplemental information

Supplemental text: The supplemental text is a readable explanation and elaboration of the subject found in the question or requirement. The text is typically taken from the Standard itself. So questions may exist that do not have supplemental information if they were not included in the Standard. If a set of questions was taken from a single long requirement, the supplemental text may be repeated for multiple questions.

Comments Section

CSET allows the user to add comments to any assessment question or requirement during the assessment process. The figure below describes the comment process.

The screenshot shows a requirement card for 'ID.AM-1 Physical devices and systems within the organization are inventoried'. At the top right are five buttons: 'Yes' (green), 'No' (red), 'NA' (blue), 'Alt' (orange), and a flag icon. Below the requirement text is a row of six icons: a clipboard, information, comments (with a red dot), document, checklist, and lightbulb. A large text input box contains the placeholder text 'This is a comment'.

Figure: Assessment screen comments section

Comments field : The Comments button displays a red dot over the comments icon when the question or requirement has comments. This allows the user to easily see which questions have comments when scrolling through the list of questions.

The Comments text box allows the user to add comments or other textual information related to a question or requirement. Comments can be added for multiple reasons such as implementation details, reasons for marking a question for review, answer justifications, etc.

In some assessments, the Comments input text box is used on rare occasions; in others, the comments are used to record the verification method of answers. This field can be a powerful tool to support the quality of the assessment, especially when documents are also attached to support the answer using empirical data.

Documents Section

CSET allows the user to associate documents to any assessment question or requirement during the assessment process. The figure below describes the document process.

The screenshot shows a document entry screen. At the top, it says "ID.AM-1 Physical devices and systems within the organization are inventoried". Below this are several icons: a clipboard, a blue circle with an "i", a speech bubble with a red dot, a document icon, a lightbulb, and a speech bubble. To the right are four colored buttons: green ("Yes"), red ("No"), blue ("NA"), and orange ("Alt"). Below these icons, there are two rows of text: "Document Title" followed by "Test Document" and "File Name" followed by "test.txt". To the right of "test.txt" are three small icons: a magnifying glass, a trash can, and an arrow pointing right. At the bottom left is a blue button labeled "Add a document".

Figure: Documents section

Documents button : The Question Documents button displays a red dot over the Document icon when the question or requirement has associated documents. This allows the user to easily see which questions have associated documents when scrolling through the list of questions.

The Question Document List displays all documents currently associated with the selected question. It displays the document title and file name as well as the Associated Questions button, Remove Document button, and Export Document button. The File Name is the name of the physical file with its file extension.

Related Questions button

The Related Questions button opens the Related Questions window that shows all questions that the document is associated with.

The screenshot shows a window titled "Related Questions". The main content area says "This document is attached to the following questions:" followed by a bulleted list: "• Access Control #2". At the bottom left is a grey "OK" button.

Figure: Related Questions Window

Remove Document button

The Remove Document button allows the user to remove the association between a document and a question. If the document isn't associated with another question, it will remove the document from the assessment.

Download Document button

The Download Document button allows the user to download a document from the assessment so it can be reviewed. Clicking the Download Document button will save a copy of the document file to a specified location.

Add a document

Add a document : Clicking the Add Document button will open an "Open File" dialog window allowing the user to navigate to a document file to associate with the question or requirement. Once selected, the document will be displayed in the Question Document List below the Add Document button.

References Section

The References Section contains links to related source and Help documentation as seen in the figure below.

ID.AM-1 Physical devices and systems within the organization are inventoried

Yes No NA Alt Flag

Source Documents	Section
Cybersecurity Framework V 1.1	ID.AM
Help Documents	Section
NIST Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations	CM-8
Council on Cybersecurity (CCS) Top 20 Critical Controls (CSC)	1
Control Objective for Information and Related Technology V5	BAI09.01
Control Objective for Information and Related Technology V5	BAI09.02
ISA99: Industrial Automation and Control Systems Security	4.2.3.4
ISO 27001 IT Security Management Standard	A.8.1.1
ISO 27001 IT Security Management Standard	A.8.1.2

Figure: Question details references section

References button  : The References button displays all references related to the question/requirement.

There will always be at least one source document for the selected Standard. If there is more than one source, then all the sources will be shown in the list of hyperlinks under the title. If the Universal set was selected, then the source will typically be the DHS Catalog of Control Systems Security: Recommendation for Standards Developers, Version 7, often referred to as the Catalog of Recommendations or CoR. If another Standard was selected, then that Standard document would be the source. In most cases, the document will open to the section where the requirement is found.

Observations Section

The Observations Section of the question details allows the user to associate observation information with a question or requirement. The figure below shows the Question Details Observations Section.

ID.AM-1 Physical devices and systems within the organization are inventoried

Yes No NA Alt

Observation Title	Importance
Test	Low

Add an Observation

Figure: Details observations section

Observations button : The Observation button displays a red dot over the Observation icon when the question or requirement has associated observations. This allows the user to easily see which questions have observations when scrolling through the list of questions.

Add an Observation : Clicking the Add an Observation button opens the Observations Window that allows the user to enter all question observation related information.

For more information about the Observations Window, see the [Question Observations](#) help section.

Question Observations

The Question Observations window allows the user to enter information about a question or requirement that has a no answer. Any question or requirement that has been answered "No" could potentially have a observation record. The observation records provide information about the issue, potential impacts of the issue, recommendations for rectifying the issue and potential vulnerabilities related to the issue. Responsible individuals can also be assigned to observation records to be responsible for fixing the problems associated with the observation record. The figure below describes the different parts of the Question Observations window.

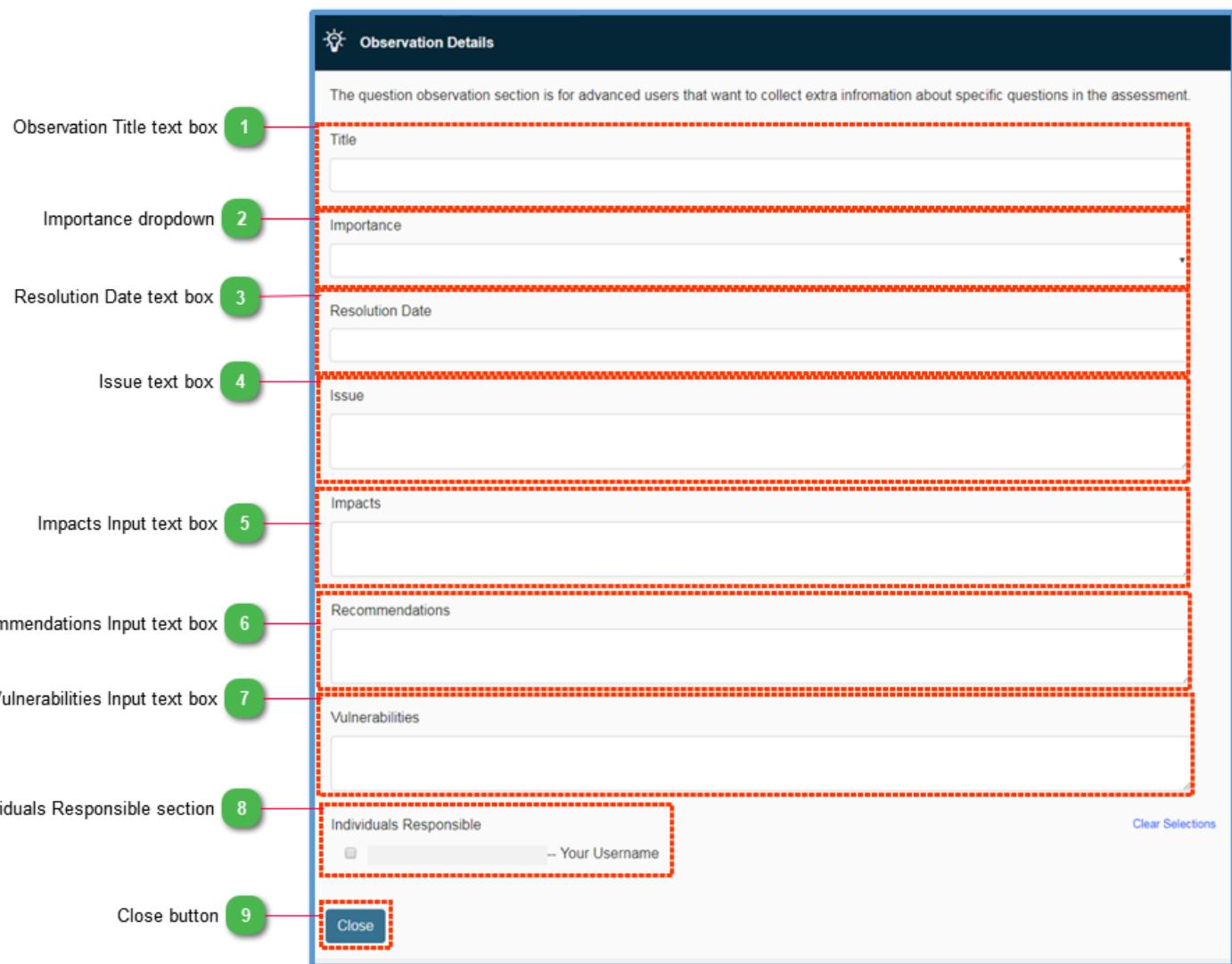


Figure: Observation details window

1 Observation Title text box

A close-up view of the 'Title' input field, which is a simple text input box labeled 'Title' above it.

The Observation Title text box corresponds to a Title or Name for the Observation record to help the user identify it.

2 Importance dropdown

Importance

The Importance dropdown allows the user to assign an importance level to the observation record. Valid values are Low, Medium, and High.

3

Resolution Date text box

Resolution Date

The Resolution Date input text box provides input for entering a date when the issue should be resolved.

4

Issue text box

Issue

The Issue input text box allows the user to define a detailed explanation of the issue or problem related to why the question or requirement was answered "No".

5

Impacts Input text box

Impacts

The Impacts input text box allows the user to define potential or real impacts that the issue may or is currently having on systems, assets, and/or procedures.

6

Recommendations Input text box

Recommendations

The Recommendations input text box allows the user to provide recommendations or steps for resolving the issues or problems defined in the observation..

7

Vulnerabilities Input text box

Vulnerabilities

The Vulnerabilities input text box allows the user to identify any known vulnerabilities on systems or assets related to the observation.

8

Individuals Responsible section

Individuals Responsible



-- Your Username

The Individuals Responsible section allows the user to assign individuals to be responsible for fixing the issues identified in the observation record. The Contacts check list will contain a list of all current contacts associated with the assessment. Selecting a contact will associate an individual to be responsible for the observation record.

9 Close button

Close

The Close button will close the Question Observations window.

Feedback Section

CSET allows the user to send feedback to both DHS and the FAA regarding questions and requirements. The figure below describes the feedback process.

The screenshot shows a requirement card for 'ID.AM-1 Physical devices and systems within the organization are inventoried'. The card includes a list of icons: a clipboard, an information icon (i), a speech bubble, a document, a bar chart, a lightbulb, and a feedback icon (a speech bubble with a red dot). Below the card is a feedback input field containing the text 'This is feedback.' At the top right are four buttons: 'Yes' (green), 'No' (red), 'NA' (blue), and 'Alt' (orange). A small flag icon is also present.

Figure: Assessment screen feedback section

Feedback field : The Feedback button displays a red dot over the icon when the question or requirement has feedback. This allows the user to easily see which questions have feedback when scrolling through the list of questions.

Users can submit their question feedback to DHS or FAA via the [Submit Feedback](#) section in the Results tab.

Question Filter

Use the Question filter to limit the Question types you see. The user can filter on answer type (Yes, No, NA, Alt, Unanswered) or added observations, comments, and marked for review.

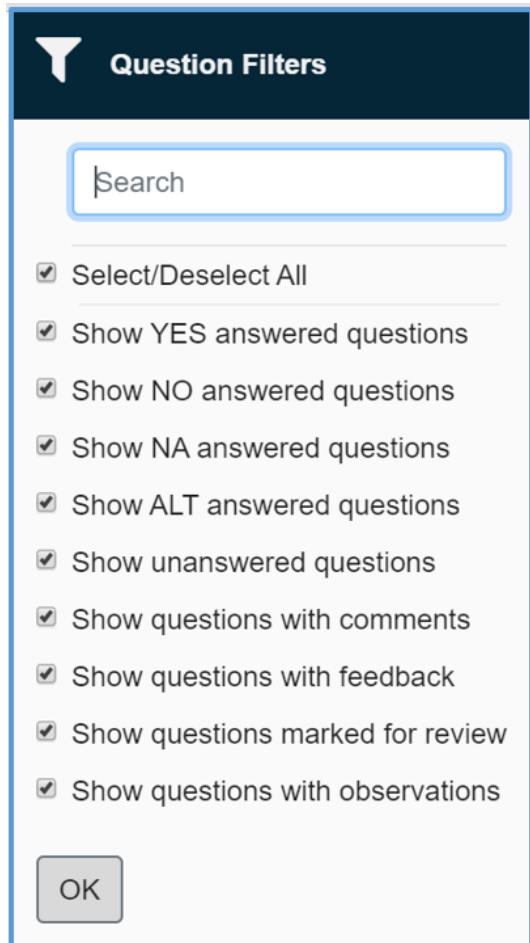


Figure: Question filter

The user can select as many filters as they would like to combine, select all, or select none.

A message will appear if there are no results to show so that the user can change their selection.

The screenshot shows the CSET application interface. At the top, there is a navigation bar with the CSET logo, a 'Tools' dropdown, a 'Resource Library' link, a 'Help' link, and a 'Your Username' dropdown. Below the navigation bar, the main menu has three tabs: 'Prepare' (disabled), 'Questions' (selected), and 'Results'. Underneath the menu, there are two mode buttons: 'Questions Mode' (selected) and 'Requirements Mode'. On the right side of the header, there are buttons for 'Collapse All', 'Expand All', and a dropdown arrow, along with a checked checkbox for 'Auto-load Supplemental'. A yellow banner at the top of the content area says 'Showing Only Filtered Questions'. Below this, a yellow warning box contains a exclamation mark icon and the text: 'There are no questions visible for the current filters or search criteria. Please change your selections and try again.' At the bottom left is a 'Back' button, and at the bottom right is a 'Next' button.

Figure: No results visible error message

Component Information

Question Information for Components

When components have been added to the network diagram the system will create a set of component default questions. If no additional action is taken, the answers to the default questions will apply to all the components in the diagram. If actions are taken, such as marking a component as unique or overriding the default, then new questions will be presented for each identified component or type. Several rules apply to the way questions are managed.

- A question will be included in the list if it maps to the component placed on the diagram. For example, a clock component may have only one question and one category listed while an application server may have ten categories and over forty questions. A variety of component types will cause all the categories to be displayed along with a large number of questions. This means that only those questions that pertain to selected components will be displayed. Questions that do not pertain to any components on the diagram will not be displayed or counted.
- You may mark any single component as unique in the diagram by clicking the checkbox labeled Has Unique Questions in the Properties popup window for the selected component. When you click this checkbox and mark it as true, CSET will add a complete set of questions related to that component type. This means that questions that were presented as component defaults will be asked again specifically for that component.
- You may override a default answer for either a component type or for a single component. The image below shows the Question Information panel for component defaults. In addition to the normal reference information, it includes a new list titled Component Types. There is an option of Override or None next to each type. To override the default answer for a specific type, simply click on the Override link next to that type.

Component Type	Override Component Answer
Firewall	Override
Router	None
Virtual Local Area Network Router	None

Figure: Question information for component defaults

You will notice the component types that are associated with this question and the Override link that allows you to enter a different answer for either a specific type or for a single component.

The None option indicates that this question pertains to this component type, but there are no instances of that type on the diagram.

Clicking Override opens the [Network Component Overrides](#) screen. Here, you answer the question for all instances of that component type. Later, you can change any single answer to match a particular device. In this example, the screen relates to overriding the default answer for an IDS.

Network Component Overrides

You may override a default answer for either a component type or for a single component. At the Question Information panel, notice the Component Types section. There is an option of Override or None next to each type. This list will vary for every question and will depend on whether the question applies to the type. To override the default answer for a specific type, simply click on the Override link next to that type. Doing so opens the screen shown by the figure below.

The screenshot shows a dialog box titled "Component Question Overrides". The text inside reads: "Change the default answers that will be automatically assigned to the component types listed below. Setting the default answer from this screen will automatically answer all component questions associated to the indicated component type." Below this, there is a table with two rows:

Component:	Database Server
Question:	Are application developers only given rights needed to develop applications and not full administrative permissions?

Below the table, there is a section titled "Specific Component Name" with two entries:

Communication Server	<input checked="" type="button"/> Yes <input type="button"/> No <input type="button"/> NA
Voice Alarm History DB Server	<input type="button"/> Yes <input checked="" type="button"/> No <input type="button"/> NA

At the bottom left of the dialog box is an "OK" button.

Figure: Network Component Overrides screen

Here, you answer the question for all instances of that component type. Later, you can change any single answer to match a particular device. In this example, the screen relates to overriding the default answer for an IDS.

There are a few items to remember when using the Override function. They are:

- Any question that you specifically answer, using either the unique checkbox on the Diagram Properties window or the override option in the Question Info screen, will take precedence over any of the component default questions.
- A new heading will be added to the Question Categories tree structure for all the cases where unique or overridden questions are designated. The corresponding question sets will be added as well.

If you have accidentally marked components as overridden or just want them to inherit the defaults later on, you can always go back to the Network Component Overrides screen and click the Clear Component Question Overrides button on the Option popup screen.

Results Section

Once standards have been selected, the network diagram has been created, and the resulting questions have been answered, it is time to analyze the results of the assessment. Two methods are available to review and analyze the results. The first uses the online Results screens and the second approach is to print the reports and review the hardcopy.

The Results section provides a method to measure security posture based on the selected Standards and the questions answered during the assessment process. The Results section uses charts and tabular data to provide a visual display of the data and at the same time allows for comparisons across categories, questions, and subject areas.

The Results sections consists of the Analysis Dashboard and charts, and the Reports. This section will describe each area.

Analysis Screen

The Analysis screen provides a quick visual view of how well the user is doing related to the user's cybersecurity posture. The Analysis screen consists of the Analysis Navigation Section, the Chart Section, and Results Navigation Section.

The figure below describes the sections of the Analysis screen.

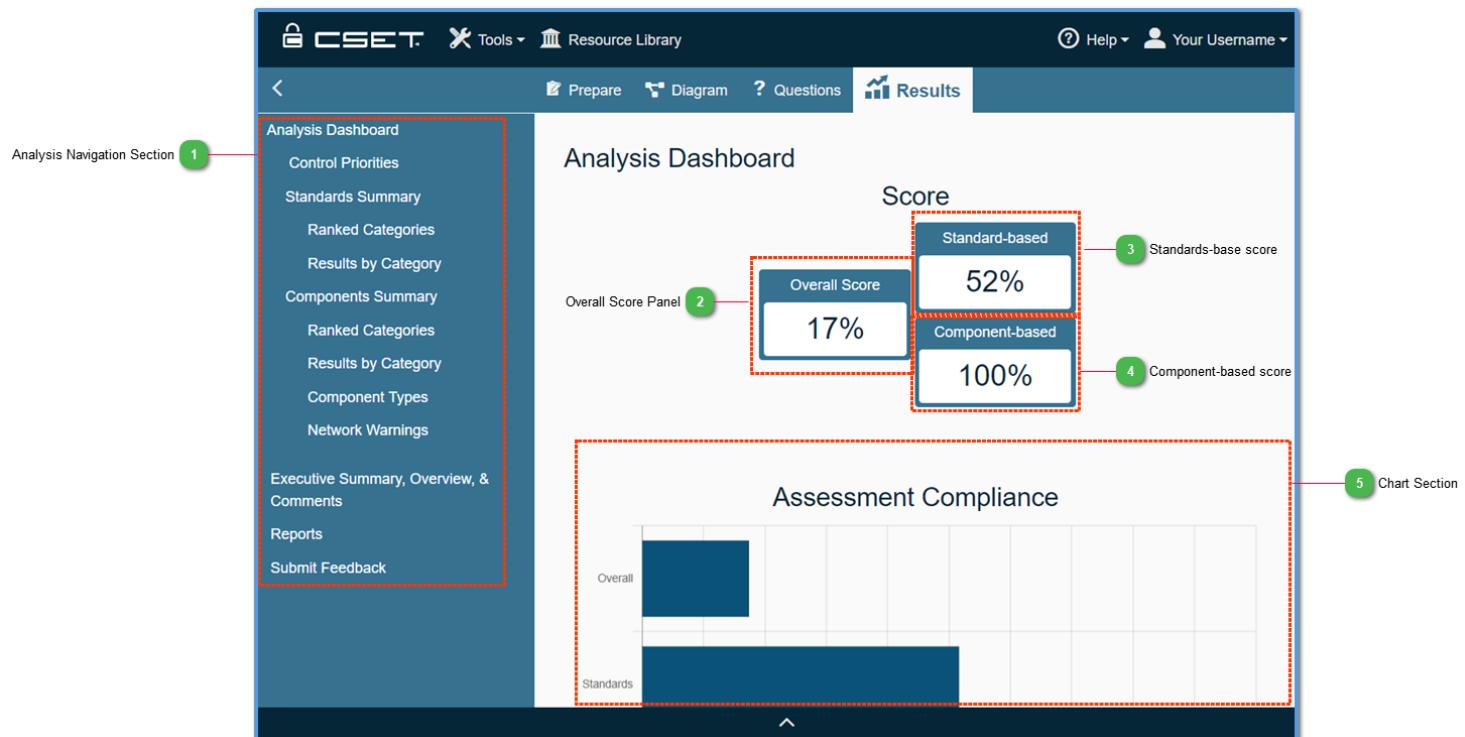


Figure: Analysis screen

1

Analysis Navigation Section

Analysis Dashboard

Control Priorities

Standards Summary

Ranked Categories

Results by Category

Components Summary

Ranked Categories

Results by Category

Component Types

Network Warnings

Executive Summary, Overview, & Comments

Reports

Submit Feedback

The Analysis Navigation section contains links for accessing the different navigation screens. Most links are divided into categories where the details can be hidden or displayed to facilitate working with the many options available.

2 Overall Score Panel

Overall Score

17%

The Overall score is calculated based on how many questions were answered "Yes" or "ALT" versus the total number of questions. The Standards value is a combination of all standards selected. The Components value represents the percentage of positive answers for all questions based on the diagram.

3 Standards-base score

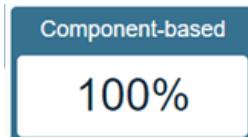
Standard-based

52%

This chart shows the combination of all the answers provided for the standards questions. If more than one standard was selected, then the chart combines the results of all the standards and displays them in a single graphic. As was mentioned above, click on the labels below the chart to turn on and off specific slices.

4

Component-based score



This pie chart shows how the component questions were answered. The answers provided for the component defaults are propagated to all the components to which the question would apply. This means that if you answer Yes to a default question that applies to only one actual component and No to a default question that applies to nine components then you would see a 10 percent Yes pie slice and a 90 percent No slice, assuming you ignore all other answers.

With this pie chart and the chart titled Standards Answers Summary, you have the ability to click on the legend to turn pie slices on and off. This can provide greater clarity if there are extremely thin slices that are not important for your review.

5

Chart Section



The Chart section is where the charts and tabular data are displayed. Generally, the user can place the mouse cursor over a chart section to see the value associated with the section of the chart. Tabular data are also available to view or export on most screens.

Dashboard in Questions/Requirements Mode

The Analysis Dashboard in Questions or Requirements mode shows four charts for quick reference. The charts displayed in the Questions/Requirements assessment mode are Assessment Compliance, Top Ranked Categories, Standards Summary, and Components Summary. The figure below provides a brief description of the Dashboard in the Questions/Requirements assessment mode.

Assessment Compliance:

This chart shows a comparison of three subjects: (1) the scoring of answers from the standard or standards if more than one has been selected, (2) the scoring of the component questions, and (3) the overall scoring for the control systems being assessed. The numbers shown are a percentage of the positive answers provided compared with the overall number of answers available. Answers marked N/A (not applicable) are not counted at all, and answers marked with an Alt or alternative are considered a positive answer like a Yes. A negative answer would be considered either a No or unanswered.

The Overall value is a combination of all the answers. The Standards value is a combination of all standards selected. The Components value represents the percentage of positive answers for all questions based on the diagram.

There is no interaction or drill down for this chart.

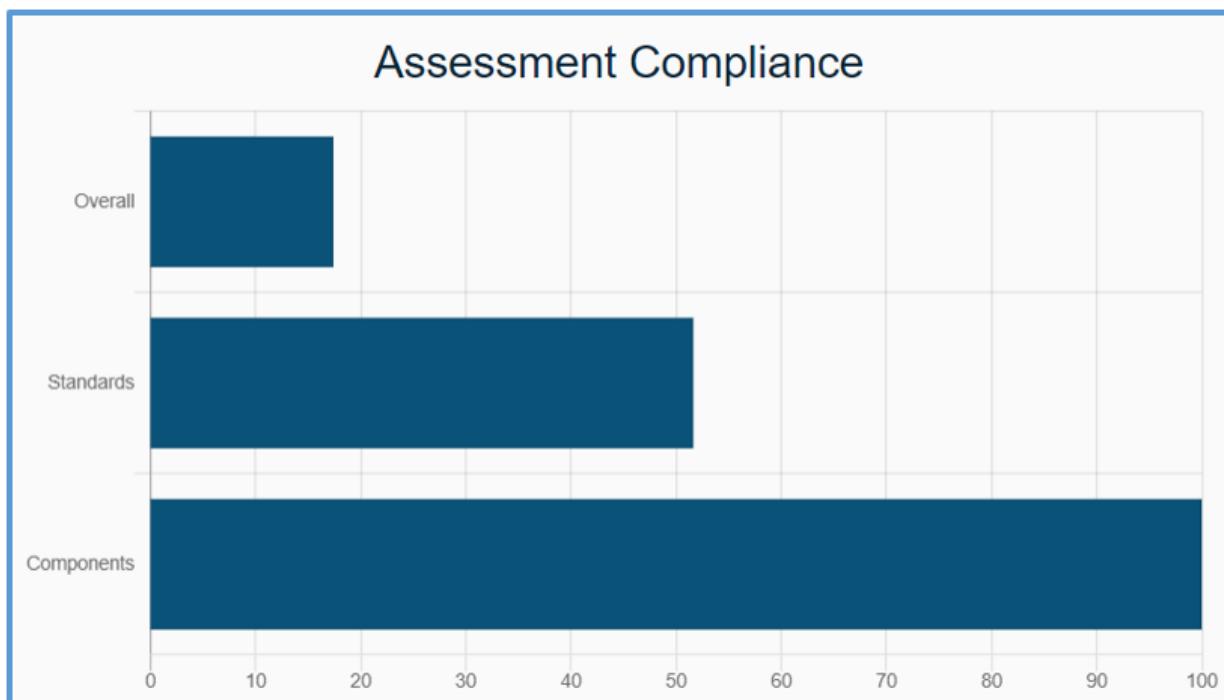


Figure: Assessment Compliance chart

Top Ranked Categories:

The Top Ranked Categories chart provides a quick look at the top six categories where the user needs to improve the most or the highest priority categories on which to focus attention first based on the assessment answers.

Top Ranked Categories

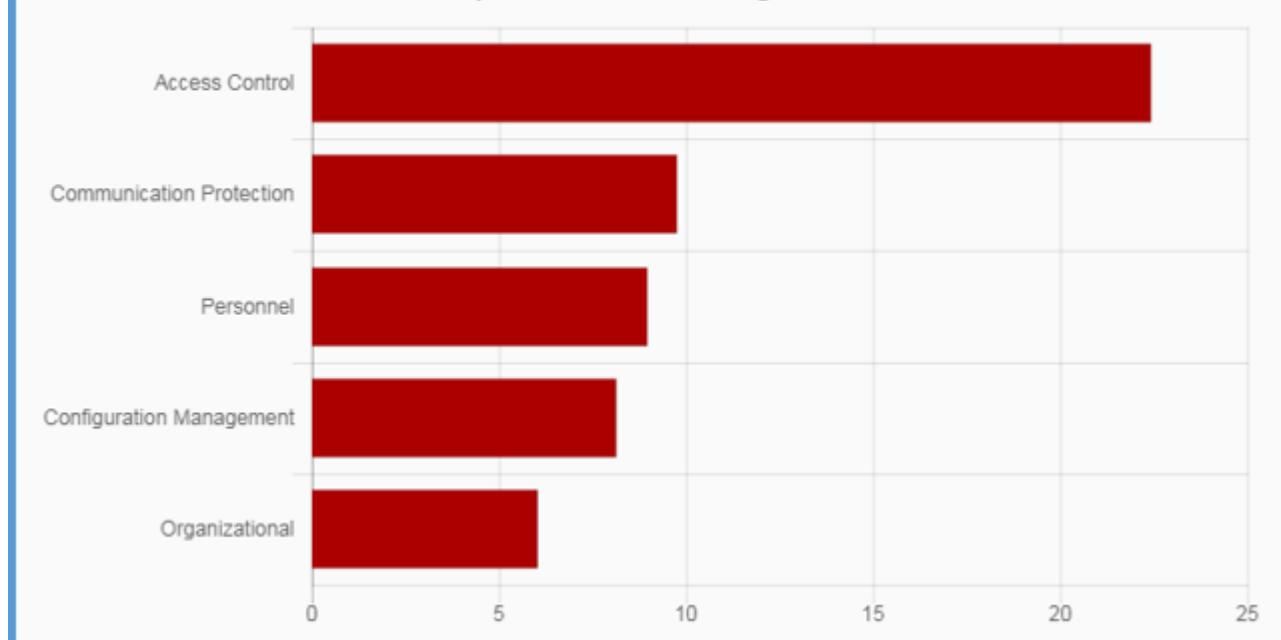


Figure: Top Ranked Categories chart

Standards Summary:

The Standards Summary chart provides a quick look at the percentages of how the user answered the Standards-based questions.

For more information about the Standards Summary chart and data, see the [Standards Summary](#) help section.

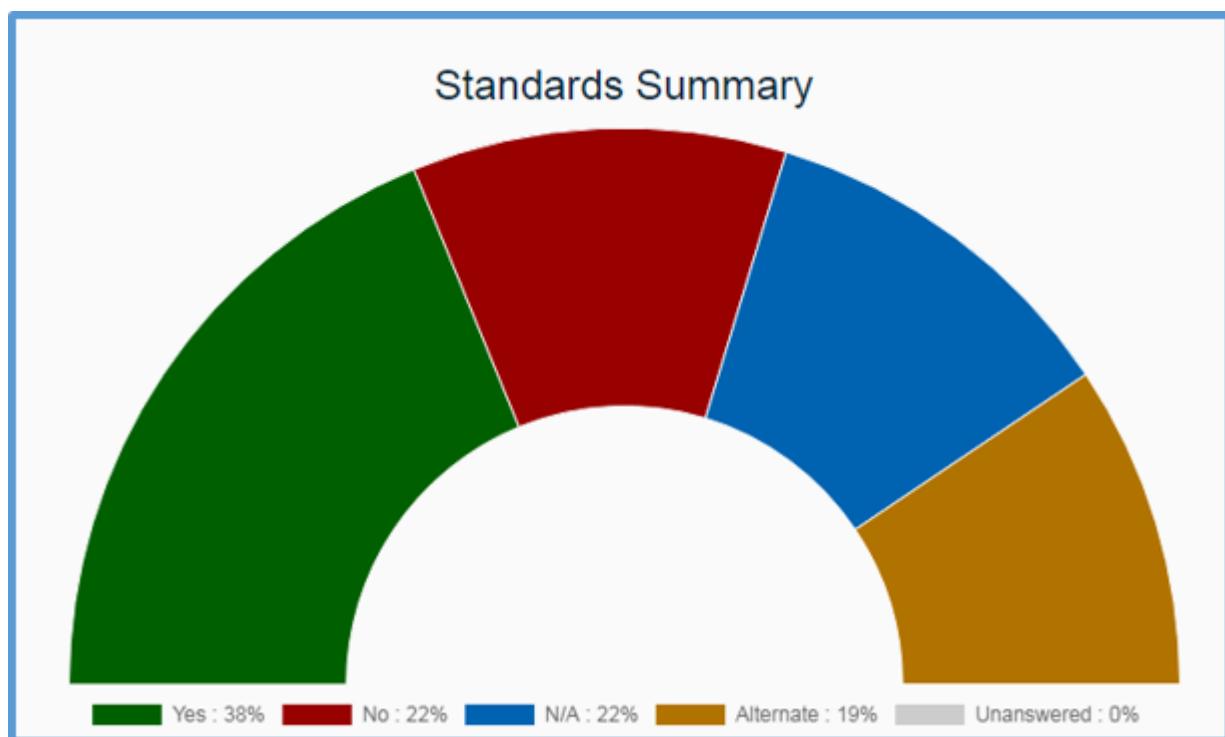


Figure: Standards Summary chart

Components Summary:

This pie chart shows how the component questions were answered. The answers provided for the component defaults are propagated to all the components to which the question would apply. This means that if you answer

Yes to a default question that applies to only one actual component and No to a default question that applies to nine components then you would see a 10 percent Yes pie slice and a 90 percent No slice, assuming you ignore all other answers.

With this pie chart and the chart titled Standards Answers Summary, you have the ability to click on the legend to turn pie slices on and off. This can provide greater clarity if there are extremely thin slices that are not important for your review.

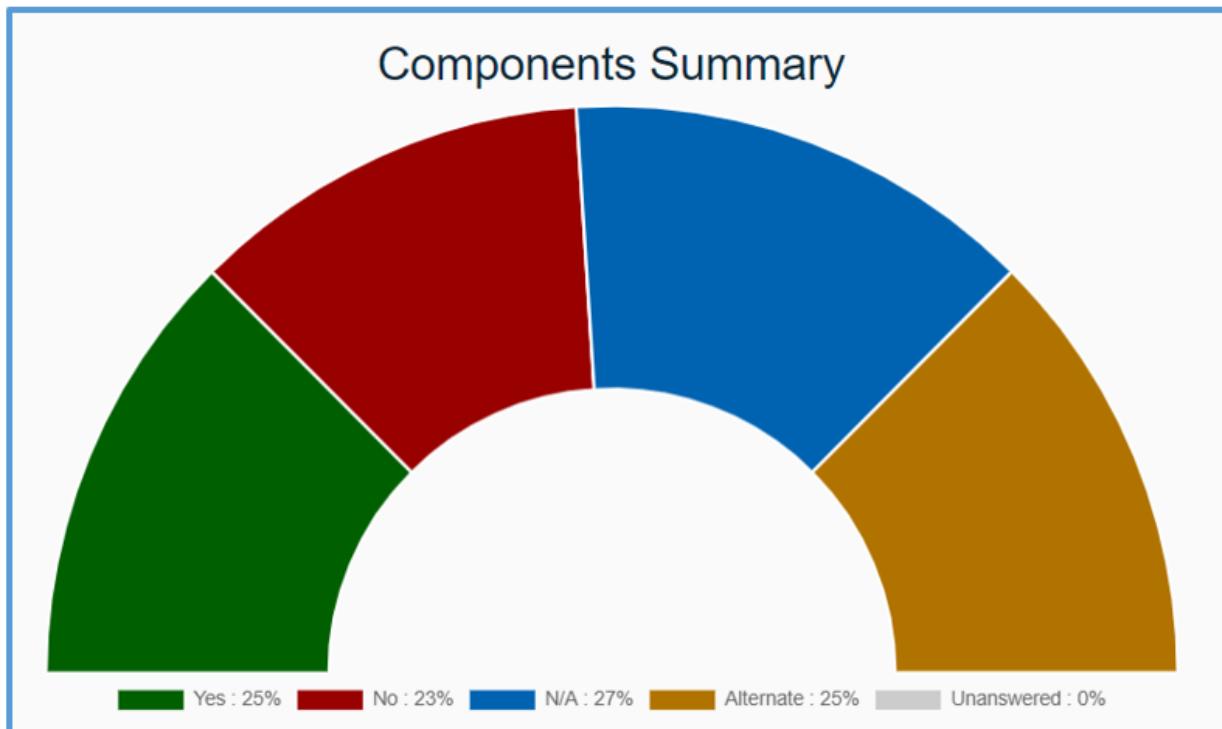


Figure: Components Summary chart

Control Priorities

Each question in the assessment where the answer had a No response or was unanswered will be ranked and displayed on the Control Priorities Screen. The information provided is intended to answer the fundamental question, "Okay, I have some problems, so what do I do first?" Based on the ranking, the answer would be, do Number 1 first, and then do Number 2, and so on until all resources have been exhausted or all the problems have been resolved.

The Control Priorities screen is shown in the figure below.

The screenshot shows the CSET interface with the 'Results' tab selected. A red box highlights the 'Control Priorities List' section. Item 1 is highlighted with a green circle containing the number 1. Item 1 details: Standard: Cybersecurity Framework, Category: Portable/Mobile/Wireless, Answer: Unanswered, Rank: 1, Question: Does the organization employ full-device encryption or container encryption to protect the confidentiality and integrity of information on organization defined mobile devices? Reference # 32. Item 2: Standard: Cybersecurity Framework, Category: Remote Access Control, Answer: No, Rank: 2, Question: Are all the methods of remote access to the system authorized, monitored, and managed? Reference # 10. Item 3: Standard: Key, Category: Remote Access Control, Answer: No, Rank: 3.

Figure: Control Priorities screen

1 Control Priorities List

Standard: Cybersecurity Framework	Category: Portable/Mobile/Wireless	Answer: Unanswered	Rank 1
Question			Reference # 32
Does the organization employ full-device encryption or container encryption to protect the confidentiality and integrity of information on organization defined mobile devices?			
Standard: Cybersecurity Framework	Category: Remote Access Control	Answer: No	Rank 2
Question			Reference # 10
Are all the methods of remote access to the system authorized, monitored, and managed?			
Standard: Key	Category: Remote Access Control	Answer: No	Rank 3

The Control Priorities list displays a list of all questions that were answered 'No' or left unanswered. The following is a description of the columns in the Control Priorities List:

Rank:

A numeric ranking of each question that was missed with #1 having the highest priority.

The ranking is based on a combination of factors that all impact the overall score. The factors include the following:

The specific weighting value assigned to each question in CSET. This weighting comes from subject matter experts with years of experience in information technology and control system cybersecurity. The questions were analyzed and assigned a weight relative to all other questions.

The weighting value of the subject area or question category. Each area was also given a weight by experts relative to all other areas. Like the question itself, it was determined that some areas are more important than others, even though they are all important to cybersecurity.

The security assurance level (SAL) of the question. Each question is linked to an assurance level. For example, a question that is associated with a Very High level would be lower in rank than one with a Low level, because it is recommended that the user work on the basic requirements before moving to those required for a higher level. A good example relates to access control. Users should implement a complex password, (or maybe even a password) before worrying about implementing system access controlled by a combination of a complex password, physical token, and biometrics. The SAL will only affect the weighting when the score is higher than a Low for the facility. Because the SAL limits the questions to only those matching the SAL value, if the score is at a Low, then the user would never see any questions that might be marked as Moderate, High, or Very High.

The component criticality value assigned by the user. In the network diagram, it is possible to change the criticality of a component from the default of Moderate to either Low or High. Those components that are most critical to the enterprise will be given priority over those that are less critical.

Standard Name:

The value in this column identifies the Standard from which the question came. This concept is especially important when using multiple Standards that have the same category names. The combination of Standard Name, Category, and # will help locate the exact question or requirement.

Category:

The title of the main question category or subject area where the question or requirement is found.

Number or #:

This column identifies the question number in the Standard and category. The content is a hyperlink that when clicked, will open the Question screen and navigate to that question. The number will be the requirement title when in the requirements assessment mode.

Question:

The text from the question or the requirement, depending on which mode was selected.

Answer:

This is the answer selected when completing the assessment.

The data can be sorted by clicking its corresponding column header but it is recommended to keep the questions in Ranked order and address them accordingly.

Standards Analysis

The Standards Analysis section of the Analysis Navigation panel displays charts and tabular data based on answers to questions for the selected Standards. Standards Analysis contains analysis screens for Summary, Ranked Categories, and Results by Category that will be described in the following sections.

Standards Summary

The Standards Summary Single Standard screen shows summary information related to the results from the answers to the single Standard that was selected at the Standards screen during the start of the assessment. The chart and tabular data displayed will correspond to a single Standard only.

The data displayed corresponds to answers to questions associated with only the selected Standard and does not include data related to components on the network diagram.

The chart shows the percentage of all Yes, No, NA, Alternate, and Unanswered questions for the selected Standard. The tabular data show the Answer in the first column. The second column indicates the number of the indicated answer, the third column shows the overall total number of questions, and the final column shows the percentage of the number for the total.

Answer	Number	Total	Percent
Yes	88	347	25%
No	101	347	29%
Not Applicable	55	347	16%
Alternate	103	347	30%
Unanswered	0	0	0%

Figure: Standards summary table

The Standards Summary Single Standard screen is shown in the figure below.

<

Prepare

Diagram

Questions

Results

Analysis Dashboard

Control Priorities

Standards Summary

Ranked Categories

Results by Category

Components Summary

Ranked Categories

Results by Category

Component Types

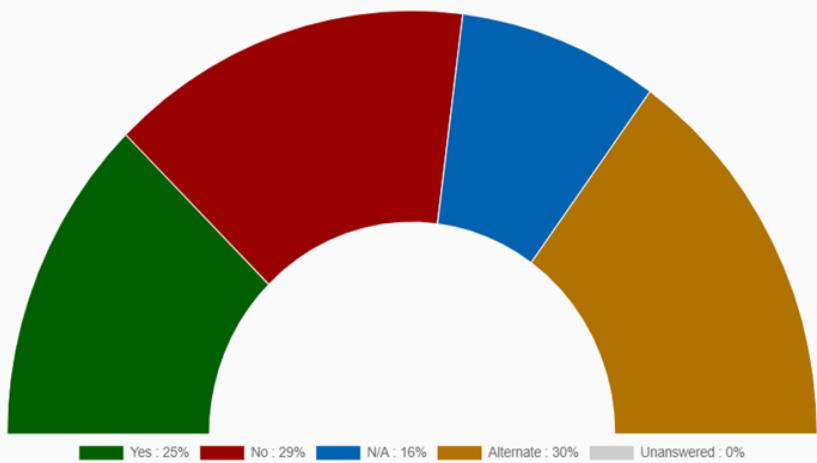
Network Warnings

Executive Summary, Overview, & Comments

Reports

Submit Feedback

Standards Summary



Answer	Number	Total	Percent
Yes	88	347	25%
No	101	347	29%

Figure: Standards Summary single standard

Ranked Categories

The Ranked Categories screen shows a list of all main categories ranked in order of the categories that should be prioritized based on how the questions were answered. Only answers from the selected Standards are included on this screen. Diagram component answers are not included. The chart shows the categories ranked in order of importance.

This screen highlights the categories that need the most attention for failed Standards based questions. Unlike other analysis screens that highlight the positive answers, this screen and the associated data show what categories or areas are weakest and what needs the most attention. In other words, the longer the bar in the chart, the worse the score in that area.

The Data Tab contains the tabular data of the categories that match the bars on the associated chart. There are five columns in the tabular data:

Category:

The categories are taken from the list of categories associated with the selected Standards. If multiple Standards are selected then this list is made up of the universal categories. Questions from a single Standard use the categories from that Standard.

Rank:

The Rank column corresponds to the size of the bar on the chart and is an importance weighting.

For more information about how categories are ranked, see the [Category Rankings](#) help section.

Failed:

The Failed count shows the number of negative answers determined by either a No or Unanswered answer. The total number of questions does not include questions marked as not applicable.

Total:

The Total indicates the total number of questions within the indicated category.

Percent:

This column is the number of failed answers divided by the total number of questions to get the percentage.

The Ranked Categories screen is shown in the figure below.

<

Prepare

Diagram

Questions

Results

Analysis Dashboard

Control Priorities

Standards Summary

Ranked Categories

Results by Category

Components Summary

Ranked Categories

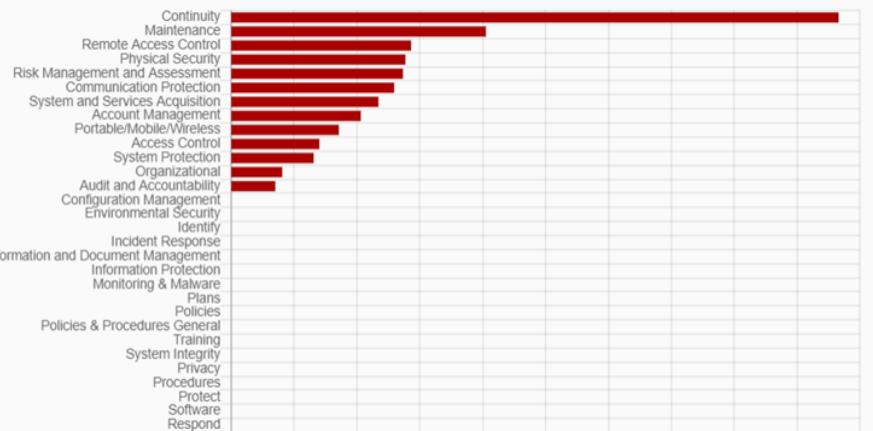
Results by Category

Component Types

Network Warnings

Executive Summary, Overview, & Comments**Reports**

Submit Feedback

Ranked Categories

Category	Rank	Failed	Total	Percent
Continuity	1	29	35	9.66%
Maintenance	2	9	14	4.05%

**Figure: Ranked Categories screen**

Results by Category Single Standard

The Results by Category Single Standard screen shows the positive results of how the user performed on the assessment organized by the category in which the questions are grouped. The results are based on questions from a single Standard selected at the Standards screen during the start of the assessment. The chart and tabular data displayed will correspond to a single Standard only. If multiple Standards are selected, the [Results By Category Multiple Standards](#) screen is displayed. The data displayed also do not include data related to components on the network diagram.

The chart displayed is a bar chart and shows the percentage of passed (Yes and Alternate) answers to questions for the selected Standard grouped into categories. The Data Tab shows the Category in the first column. The second column indicates the number of passed answers for the indicated category, the third column shows the total number of questions in the category, and the final column shows the percentage of the passed answers over the total.

The Results by Category Single Standard screen is shown in the figure below.

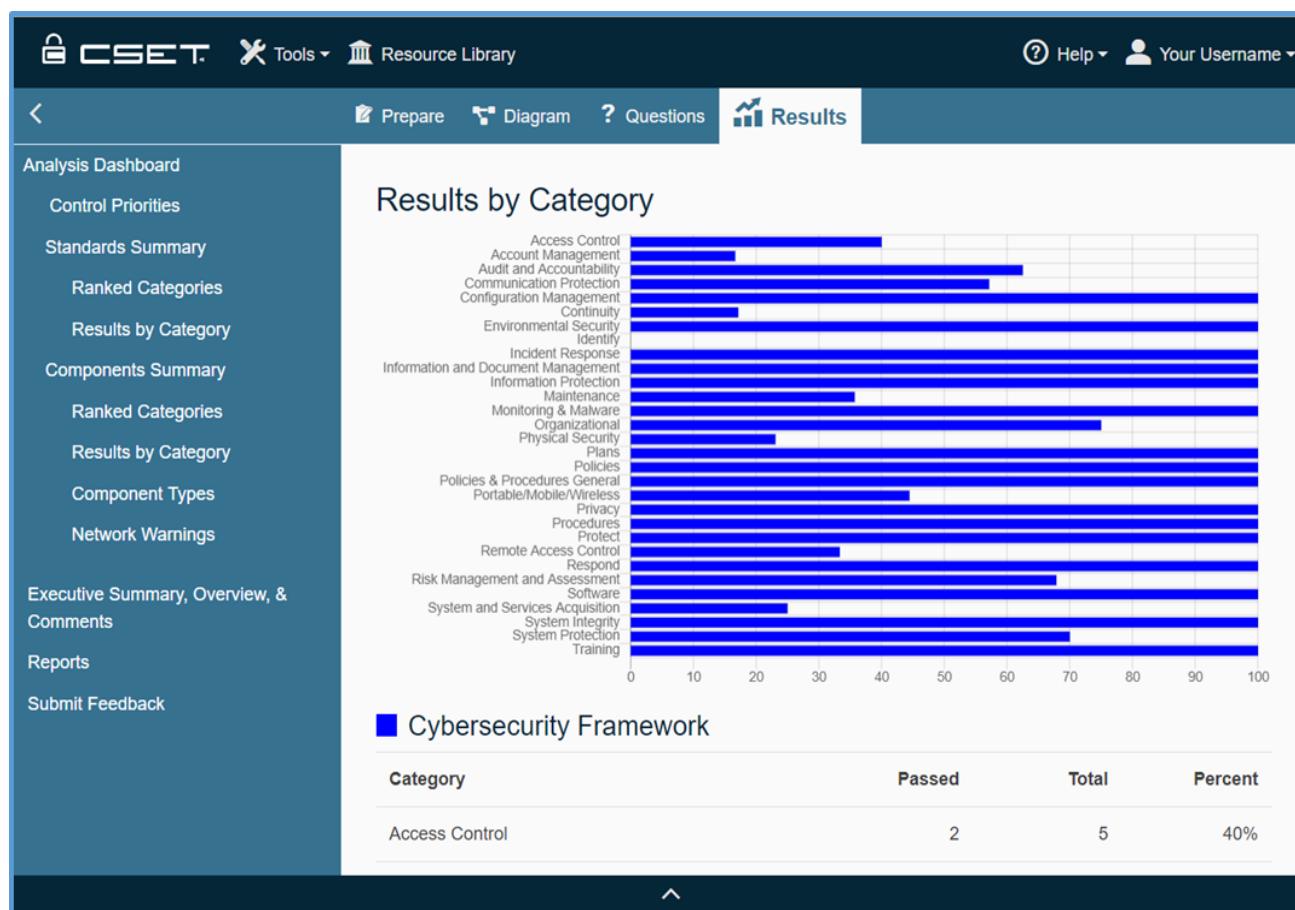


Figure: Results by Category single standard

Results by Category Multiple Standards

The Results by Category Multiple Standards screen shows the positive results of how the user performed on the assessment organized by the selected Standards as well as the category in which the questions are grouped. The results are based on questions from multiple Standards selected at the Standards screen during the start of the assessment. The chart and tabular data displayed will correspond to multiple Standards. If a single Standard is selected, the [Results By Category Single Standard](#) screen will be displayed. The data displayed also do not include data related to components on the network diagram.

The chart displayed is a multiple bar chart. For each category, the chart displays a bar for each selected Standard. Each bar shows the percentage of passed (Yes and Alternate) answers to questions for the indicated Standard. The Data Tab shows multiple tables, one for each Standard, with the Category as the first column. The second column indicates the number of passed answers for the indicated category, the third column shows the total number of questions in the category, and the final column shows the percentage of the passed answers over the total.

The main CSET window may need to be maximized in order to read the chart appropriately.

The Results by Category Multiple Standards screen is shown in the figure below.

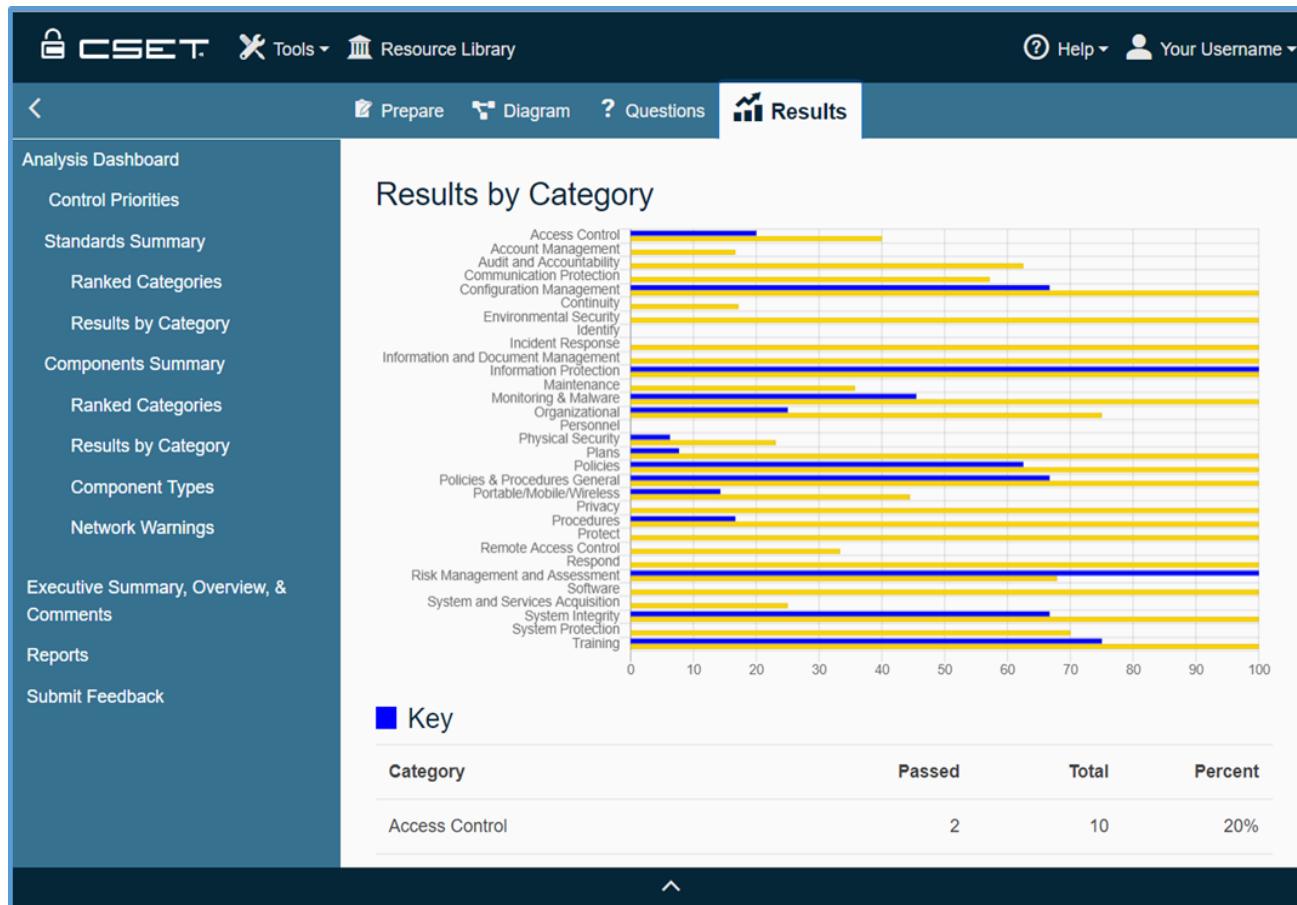


Figure: Results by Category multiple standards

Category Rankings

Each Standard has an overall defined risk. This overall risk is determined from the number of questions and the weight of each question. The weights of questions have been determined by cyber security experts. If all questions have been completely failed then the ranked category bar charts will show that the user is at 100% of the risk defined by the Standard as seen in Figure: Ranked Categories with 0%. If about half the questions were answered yes, then the graph would only show the user at 50% of the overall risk as seen in Figure: Ranked Categories with 50%. See the two graphs below.



Figure: Ranked Categories with 0% of account management questions passed



Figure: Ranked Categories with 50% of account management questions passed

Note that the x-axis is different between Figures Ranked Categories with 0% and Ranked Categories with 50%. Otherwise the graphs look about the same. The x-axis changes because the proportions of risk are the same. According to this Standard, the Monitoring and Malware controls consume about 2/3 of the risk that Account Management does. However, if we go back and answer a great majority of Account Management questions as Yes then we obtain the chart in Figure: Ranked Categories with 100%.

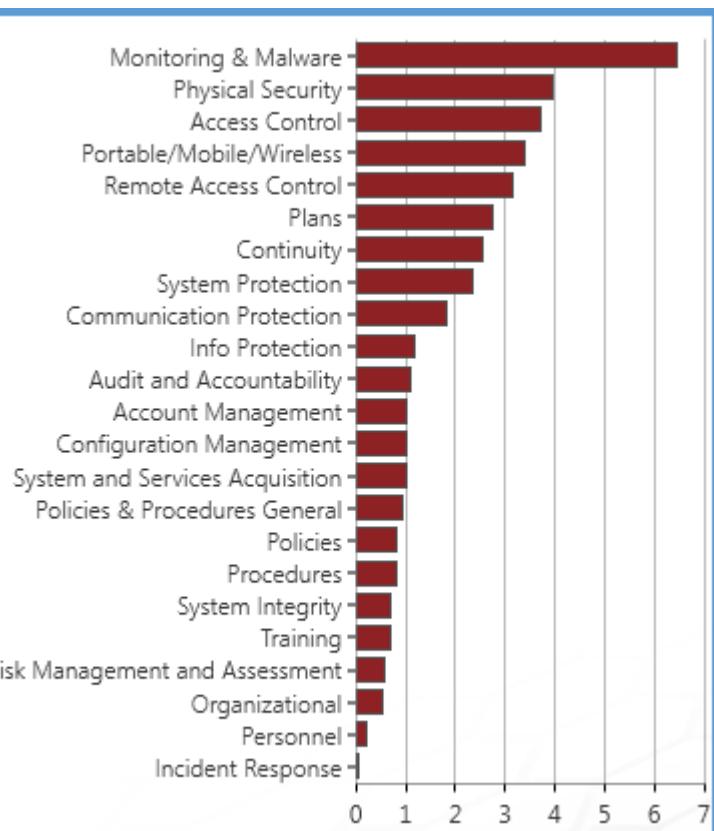


Figure: Ranked Categories with 100% of account management questions passed

Now the risk accounted for from the Account Management section is only about 1% of the original risk defined by this Standard. Note that Monitoring and Malware still Accounts for about 6% of the overall risk as it did above.

Components Summary Screen

The Components Summary screen shows summary information related to the results from the answers to the Component Default/ Component Override questions that was selected by the symbols included in the network diagram.

The data displayed corresponds to answers to questions associated with components on the network diagram and does not include data related to the selected Standard.

The chart shows the percentage of all Yes, No, NA, Alternate, and Unanswered questions for the Components. The tabular data show the Answer in the first column. The second column indicates the number of the indicated answer, the third column shows the overall total number of questions, and the final column shows the percentage of the number for the total.

The Components Summary screen is opened from the Analysis screen as shown in the figure below.

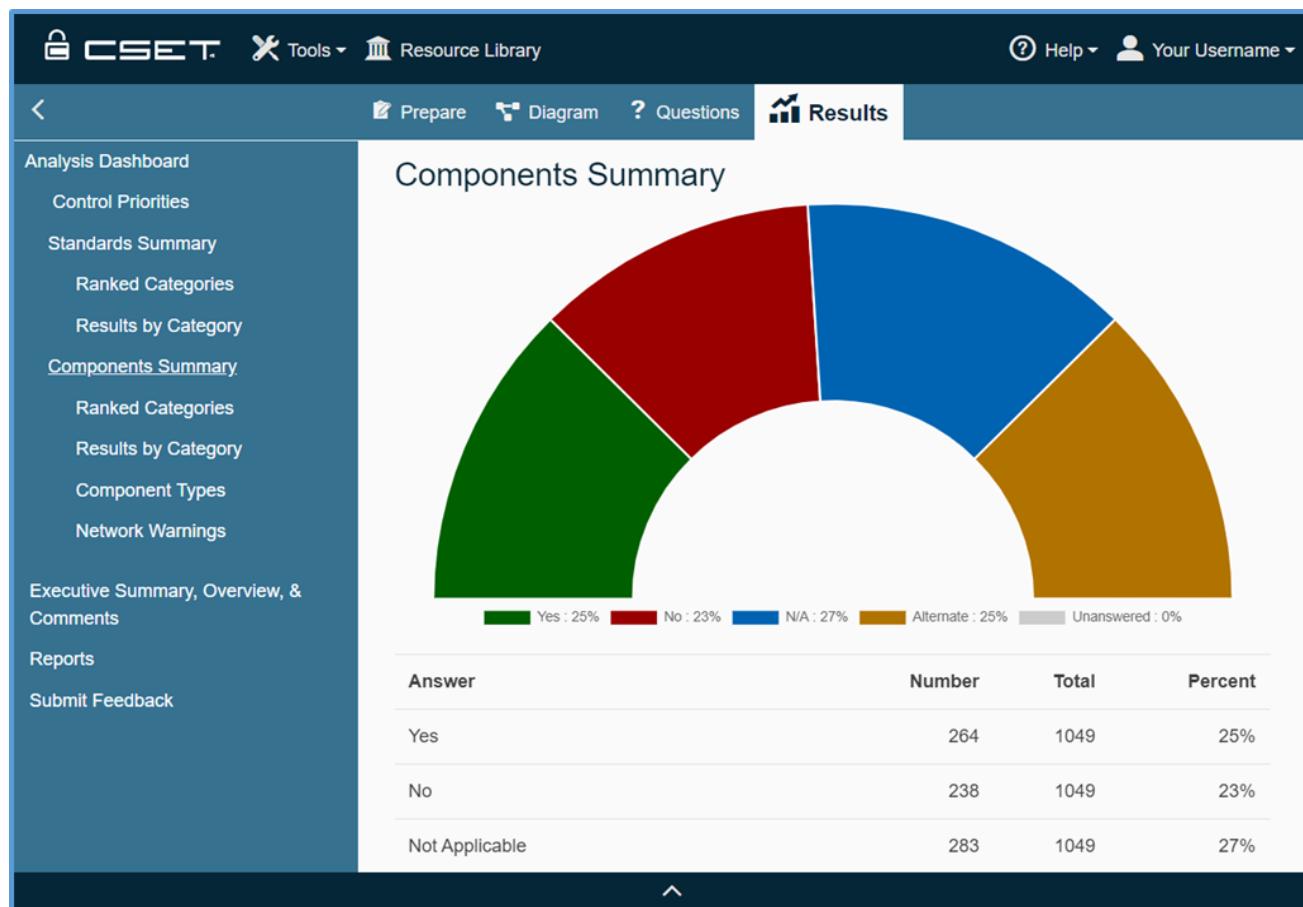


Figure: Analysis screen Components Summary

Ranked Categories

Clicking the Ranked Categories chart within the Components Summary section will then display the figure below.

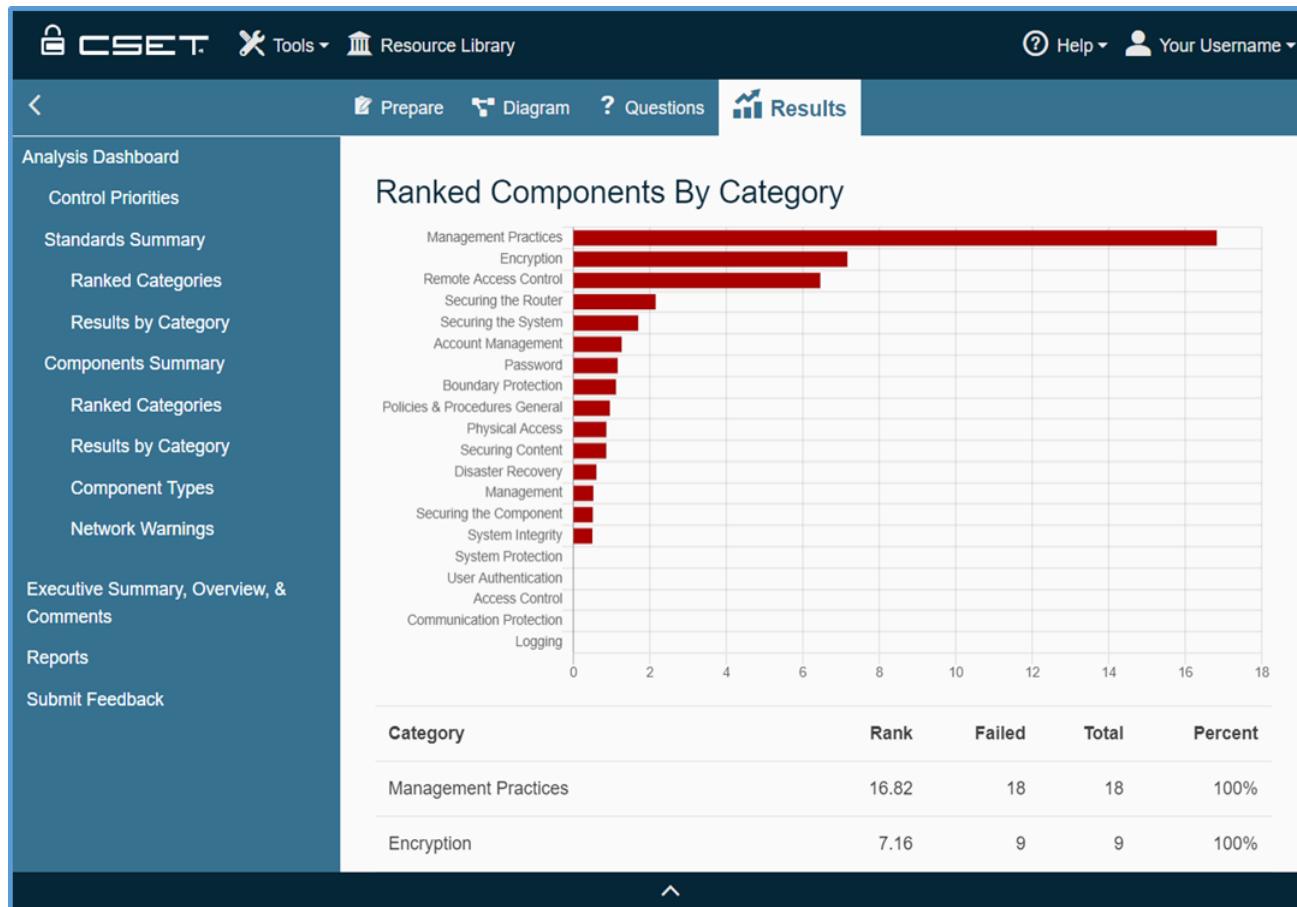


Figure: Ranked Components by Category screen

The chart shown under Components by Category provides a picture of how all the components combined scored in each topic area or category. The topic is listed as a label for each bar in the chart, and the bar length shows the percentage of positive responses as compared with all possible responses. Keep in mind that the default answers will be propagated to all the components associated with that question. For example, if you answered Yes to a single question that was linked to 50 actual components on the diagram, then the system would see that as 50 Yes answers.

The grid underneath the chart shows the summary counts of how the questions were answered.

Below the summary is a table showing the details for each category. The name of the category is first listed in the row, followed by the number of each answer, then the total number of questions, and finally the percent correct. The percent on the bottom grid will match and support the bar length and percentage number on the chart.

Results by Category

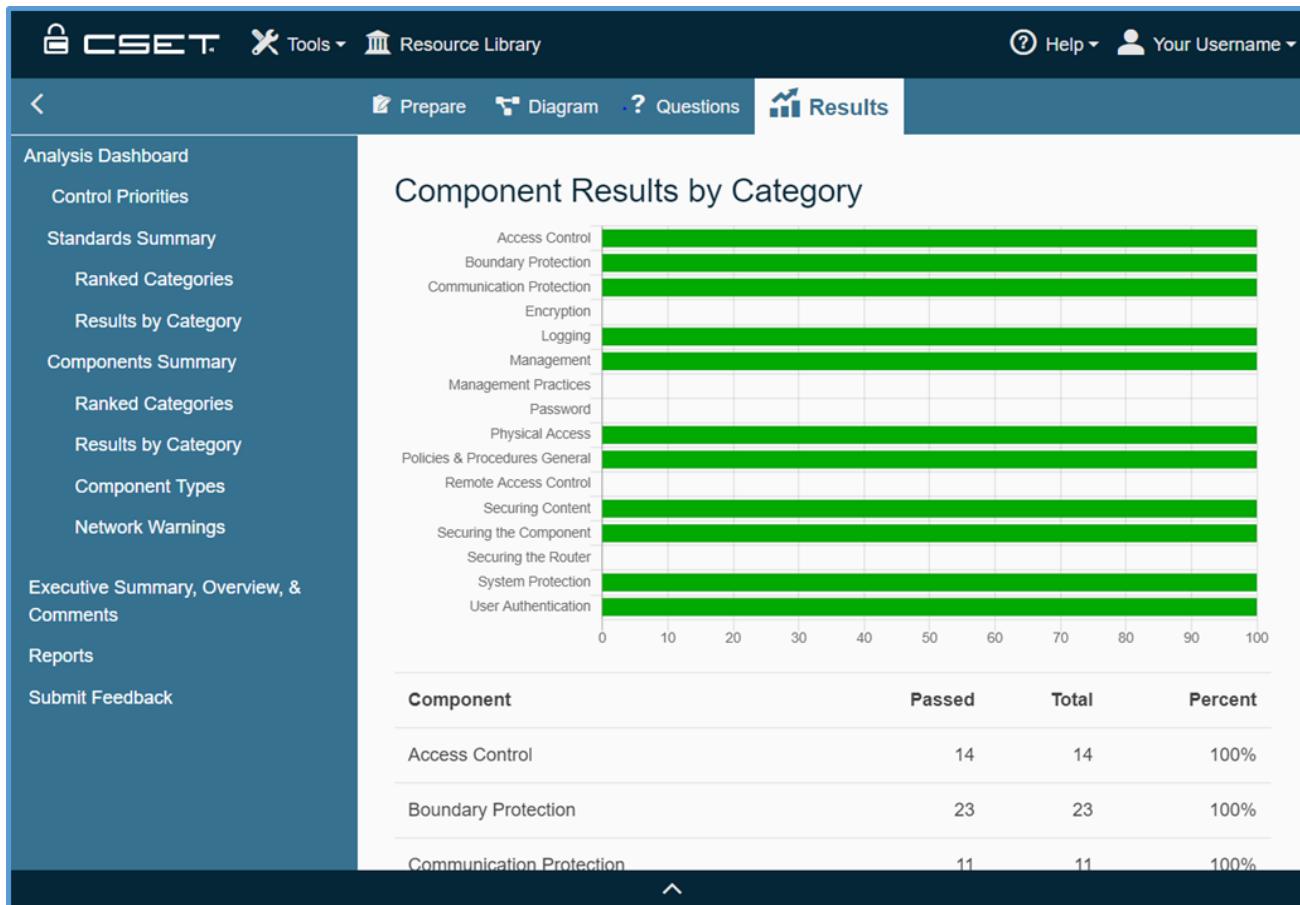


Figure: Results by Category screen

The chart shown under Components by Category provides a picture of how all the components combined scored in each topic area or category. The topic is listed as a label for each bar in the chart, and the bar length shows the percentage of positive responses as compared with all possible responses. Keep in mind that the default answers will be propagated to all the components associated with that question. For example, if you answered Yes to a single question that was linked to 50 actual components on the diagram, then the system would see that as 50 Yes answers.

The grid underneath the chart shows the summary counts of how the questions were answered.

Below the summary is a table showing the details for each category. The name of the category is first listed in the row, followed by the number of each answer, then the total number of questions, and finally the percent correct. The percent on the bottom grid will match and support the bar length and percentage number on the chart.

Component Type

In this chart, all the different answers are combined for all components of a type, regardless of whether they were answered by default or as a unique component. As mentioned earlier, remember that the default answers will be propagated to all the components associated with that question.

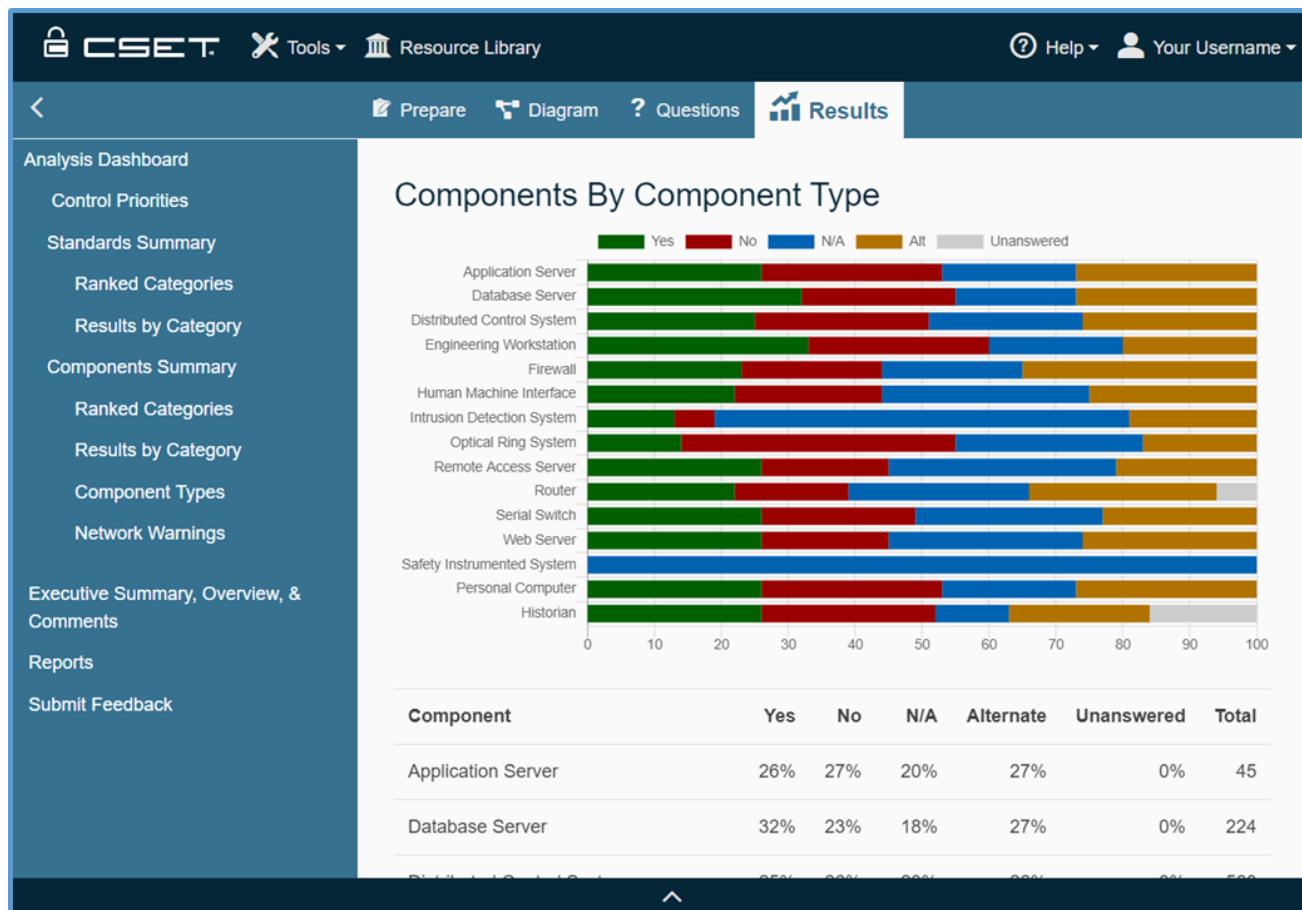


Figure: Component Types chart

Only the types that were included in the network diagram will be displayed on this chart.

Below the chart is a grid with detailed numerical data that supports the chart. The component type is listed first and matches the types shown in the chart above. The next column shows the number of components of a type that are present on the diagram. The next fields are the number of each answer with a total that is calculated by multiplying the total number of components with the number of questions per component.

There may be situations where you could have two components of the same type and the number of questions is an odd number. This happens when each component is in a different zone that has different security assurance level (SAL) values. For example, a component in a zone with a Low SAL may have 4 questions presented while the same component in a High SAL may have 7 questions. In this case the total number of questions would be 11 for the two components of the same type.

Network Warnings

The Network Warnings button on the Analysis screen provides access to a list of all network architecture warning messages found on the network diagram.

The screenshot shows the 'Network Warnings' section of the CSET interface. On the left, a sidebar lists various navigation options. The main content area is titled 'Network Warnings' and contains a list of three items, each with an identification number and a detailed description. At the bottom, there are 'Back' and 'Next' buttons.

ID	Network Warnings
1	The subnet should have an IDS (Intrusion Detection System) or IPS (Intrusion Prevention System) inline to confirm that the configuration of firewall, External Firewall, is correct and that malware has not been able to penetrate past the firewall.
2	The subnet should have an IDS (Intrusion Detection System) or IPS (Intrusion Prevention System) inline to confirm that the configuration of firewall, Firewall, is correct and that malware has not been able to penetrate past the firewall.
3	The component, Firewall, has multiple interfaces where the subnets of those interfaces carry traffic of different SALs. If the component is compromised, the critical traffic could be visible from the less protected network.

Figure: Network Warnings screen

When you click on the Network Warnings button, the system opens the Network Warnings screen.

This screen displays the identification number associated with the red circle on the network diagram and the message for the warning.

The warning messages can also be seen in the diagram itself by enabling the Analyze Network functionality and clicking on the red circle to show the warning text.

Reports Section

After the assessment is complete the user can generate and print reports of the results.

The intent of the reporting function is to provide a way to print and publish assessment information, including summary charts and lists. It also provides a hardcopy of the results to be used in meetings, for communications to management, and as a way to assign tasks to technical staff. Combined with the online analysis, these reports can help the user clearly understand where weaknesses are and where improvements should be made.

This section will describe how to use the Reports Screen.

Executive Summary, Overview, and Comments Screen

The Executive Summary, Overview, and Comments screen allows the user to add executive level information for display on the Executive Summary report. As well as, a high-level description of the assessment and any relevant comments to be displayed on the reports.

Some default text is provided on the Executive Summary screen; however, the user should replace that text with actual summary information that captures the highlights of the assessment as seen in the figure below.

The screenshot shows the CSET interface with the 'Results' tab selected. The left sidebar contains a navigation menu with items such as Analysis Dashboard, Control Priorities, Standards Summary, Ranked Categories, Results by Category, Components Summary, Ranked Categories, Results by Category, Component Types, Network Warnings, Executive Summary, Overview, & Comments, Reports, and Submit Feedback. The main content area has two sections: 'Executive Summary' and 'Overview'. The 'Executive Summary' section contains a placeholder text about cyber terrorism and standards. The 'Overview' section has a text input field with a placeholder 'Please provide a description of the assessment process and work performed.'

Figure: Executive Summary screen

Report Builder

The Report Builder screen is shown in the figure below.

The screenshot shows the 'Report Builder' screen within the CSET application. The left sidebar contains a vertical list of navigation links: Analysis Dashboard, Control Priorities, Standards Summary, Ranked Categories, Results by Category, Components Summary, Ranked Categories, Results by Category, Component Types, Network Warnings, Executive Summary, Overview, & Comments, Reports, and Submit Feedback. The main content area is titled 'Report Builder' and contains a brief description: 'Create your final reports. You can add descriptions, comments, and an executive summary to your reports. You can also specify comments and descriptive text.' Below this description is a list of report types: Executive Summary, Site Summary Report, Site Cybersecurity Plan, Site Detail Report, and Observations Tear-Out Sheets. At the bottom of the main content area are two buttons: 'Back' on the left and 'Next' on the right. The top of the screen features a header with the CSET logo, a 'Tools' dropdown, a 'Resource Library' link, a 'Help' link, and a 'Your Username' dropdown.

Figure: Report Builder screen

To generate a report click on the specific report link on the Report Builder screen. The report will open in a new tab.

Executive Summary: The Executive Summary option produces the Executive Summary Report. As the name implies, it is designed for an executive level audience. The person receiving the report may hold any title; however, the intent is to provide limited graphical and high-level, summary information that can be understood quickly.

This report is limited to around five or six pages and does not include any detailed information beyond listing the top categories and areas of concern. It includes the textual Executive Summary information available on the [Executive Summary Screen](#). It also includes the High Level Assessment Description, which is found on the [Comments & High Level Description screen](#).

Site Summary: The Site Summary option produces the Site Summary Report. The intended audience for this report is a technical manager or supervisor who is responsible for directing the implementation of the recommendations. The report includes everything in the Executive Report plus additional charts at a more detailed level. It also includes the network diagram and a list of all the questions in the assessment that were not positively answered. An important feature is the ranking of the missed questions. Each question is ranked sequentially from one to the total number of questions.

The question ranking is determined by a formula that takes into consideration the weighting of each question, the weighting of each category, and the security assurance level (SAL) associated with that question. All questions

in CSET have been assigned a unique weighting relative to one another. The categories have been weighted as well. These assignments were determined by subject matter experts and are based on their recommendations. The SAL that is assigned to a question is also considered in the formula. For example, all other things being equal, if Question A has a SAL of High and Question B has a SAL of Low, then Question B would rank higher in the list than A. The recommended ranking would encourage addressing basic requirements before addressing the more difficult ones.

The rankings are intended to address the question, "What should I work on first?" It is recommended to start with the question ranked Number 1 and work down the list based on available resources and the cybersecurity plan.

Detail Report: This option will generate the Site Detail Report. The intended audience for this report is the implementers of change in the organization as it provides the details needed to make the necessary resource allocations and commitments to improve the cybersecurity of the facility or site.

Security Plan: The Security Plan option produces the Site Cyber Security Plan template. It provides an overview of system security requirements and describes the controls in place or planned to meet those requirements.

The plan includes several sections found in the Site Summary Report but the bulk of the report is a list of all assessment questions and their answers presented in a control-focused format. Thus, the report provides an overview of the cybersecurity requirements and the status for the facility.

Discoveries Tear Out Sheets: The Discoveries Tear Out Sheets option produces a list of all discoveries identified on specific questions during the assessment. Contacts can be assigned to each discovery record and the printed report will allow for easy distribution of assignments to address each discovery or potential issue.

Executive Summary Report

The Executive Summary Report is designed for an executive level audience. The intent is to provide limited graphical and high level, summary information that can be understood quickly.

This report is limited to around five or six pages and does not include any detailed information beyond listing the top categories and areas of concern. It does include the textual Executive Summary and Description of Assessment text that was entered by the user at the Information screen. Some default text is provided; however, the default text should be replaced with actual summary information that captures the highlights of the assessment.

The Executive Summary Report has a fixed set of sections that are all generated when the report is created. Each of the sections in the report will be discussed below.

Title Page: Each of the reports has a cover page that is unique to the report type. Each includes the assessment name that is taken from the Information screen in the tool, the date that was entered in the Assessment Date field, and the name of the person that was entered in the Principal Assessor/Name field in the Information screen.

Description and Summary: This is the first page with content and shows a summary look at the Standards, network components, and overall compliance based on answers to questions in the assessment. It also includes the description of the assessment and the executive summary text that was entered in the Information screen.

When CSET is installed, the Executive Summary field has generic text included as a starting point; however, once the assessment is complete, the included text should be replaced with executive summary text that is specific to the actual assessment results.

Standards Summary: The Evaluation Against Selected Standards displays several items. It first identifies the Standards that were used in the evaluation. It then shows in pie chart format the combined breakout of answers for the selected Standards. The bar chart provides the greatest level of detail and indicates the overall scoring in each question category for the selected Standards.

Because more than one Standard may be selected, the categories are not specific to a single Standard. Instead, the categories are taken from a common list that applies to all.

Component Analysis: Like the previous page, this also provides summary information but for the set of components in the network diagram. On this page, the user would see the combined summary of answers for all components in the pie chart. This is basically a percentage of all answers for all the combined component questions. The lower bar chart shows the scoring for each component type.

Also reported is the number of warnings found by the basic network analysis. These are the red circle warnings that are shown in the diagram when the Analyze Network function has been enabled.

Areas of Concern: The final section of the Report shows the top subjects or categories and top questions of concern.

The top questions and categories are based on the ranked order of both, and the full lists can be found in the Site Summary and the Site Detail reports. Both lists on this page have been limited to only the top five. The intent is to give a quick picture of what is recommended to be addressed first.

If the user selected the Requirements or Cybersecurity Framework approach to the assessment, this section will deal with the requirements of concern, and the list will be the actual requirement text.

Ranking: The list is based on a formula that includes the number of missed questions, the weighting given to each of those questions, the weighting assigned to the question category or area, the SAL for the question, and the criticality assignment for a component that was included in the diagram.

All the parameters are factored together. Each question is ordered in the list from the question the user should work on first at the top to the question or requirement that should be addressed last listed on the bottom.

Site Summary Report

Selecting the Site Summary option produces the Site Summary Report. The intended audience for this report is a technical manager or supervisor who is responsible for directing the implementation of the recommendations. The report includes everything in the Executive Report plus additional charts at a more detailed level. It also includes the network diagram and a list of all the questions in the assessment that were not positively answered. An important feature is the ranking of the missed questions. Each question is ranked sequentially from one to the total number of questions.

The Site Summary Report provides mostly summary information in the form of a variety of charts; however, it is more detailed than the Executive Summary Report and provides additional charts that the Executive Summary Report does not have.

The sections of the Site Summary Report are discussed below.

Title Page: The Title Page includes the assessment name, date, and the name of the principal assessor.

Disclaimer: The disclaimer describes the limitations for use and legalities of CSET and the report.

Advisory: The Advisory includes recommendations for using CSET for more than an approach to a robust cybersecurity plan, for the team makeup, and for protecting data. It should be read and followed.

Site Information: This section displays the text that was entered on the Information screen in the tool. It will display all the data with the appropriate labels.

Description and Summary: This is identical to the first page of the Executive Summary Report.

Standards Summary: This page is identical to the page in the Executive Summary Report.

Standards Compliance: A Standards Compliance bar chart is displayed for every Standard selected in the tool. This chart gives the percent of positive answers (either marked as a Yes or Alternative) as compared with the total number of questions in each category. Unlike the earlier combined Standard Summary, this chart uses the categories that are specific to the Standard. The title on the chart is the short name or abbreviation of the full Standard name.

Network Diagram: A scaled copy of the network diagram is included in the report. The system scales the diagram to fit on the letter-sized (8.5" × 11") page.

Component Analysis: This is the last of the common report pages and is described under the Executive Summary Report section.

Component Compliance by Subject Area: Like the standards, this chart shows the percentage of combined questions that were positively answered in each subject area. Because the components are not linked to any specific standard, the common categories or subject areas are used.

Network Findings: This list presents the text of the warnings found by the basic network analysis.

Security Assurance Level (SAL): The Security Assurance Level page displays the results of answers and selections related to the SAL. It includes any values that were determined in the General SAL or the FIPS 199 SAL processes along with any Standard specific values like those for DoD 8500.2. When Cybersecurity Framework Mode is selected as the assessment mode, this section will be changed to display the Cybersecurity Framework Tier Determination.

Document Library: The next page shows the document titles and file names of any documents that were added to the assessment by the user. They may have been added in association with specific questions or added through the Document Library screen.

Ranked Subject Areas: The Ranked Subject Areas section shows the categories or subject areas that need the most attention. This chart is organized so that the worst areas are shown at the top and then ordered to those areas doing best at the bottom. This chart can be helpful in prioritizing what areas to work on first.

The formula for ranking these areas includes several factors such as a weighting given to each area from subject matter experts combined with the number and level of missed questions in each area.

The top five areas shown on this chart are used to populate the top categories of concern section of the Executive Summary Report.

Summary of Ranked Questions: This table includes a list of the questions that were missed presented in ranked order. It makes up the bulk of the report. This list is intended to answer the question, "What do I work on first?"

The table also presents the SALs applicable to the question. General SALs will be listed for most Standards and network components. They are Low (L), Moderate (M), High (H), and Very High (VH). If a CNSSI Standard is selected, the Confidentiality (C), Integrity (I), and Availability (A) levels will be shown. If DoD Instruction 8500.2 is the selected Standard, the Confidentiality (Conf) and Mission Assurance Category (MAC) levels will be shown. They are: Classified (C), Sensitive (S), and Public (P) for Confidentiality; MAC I, II, and III for Mission Assurance Category.

For requirements mode, the table lists the name of the Standard and the available security levels.

The top five questions on this chart are used to populate the top questions of concern section of the Executive Summary Report.

The format of the table is:

Rank #	Question/Requirement Identifier	SAL
Question or Requirement Text	Answer	

Rank#: The calculated position in the list.

Question/Requirement Identifier: The topic, category, or requirement and question number.

SAL: The SAL applicable to that question or requirement.

Question or Requirement Text: The text as seen in the Questions screen.

Answer: Why the question is listed in the table. Usually the question was answered No or left unanswered (blank). Unanswered questions should be reviewed and answered, then the report recreated.

Ranking: The list is based on a formula that includes the number of missed questions, the weighting given to each of those questions, the weighting assigned to the question category or area, the SAL for the question, and the criticality assignment for a component that was included in the diagram.

All the parameters are factored together. Each question is ordered in the list from the question the user should work on first at the top to the question or requirement that should be addressed last listed on the bottom.

The SAL of each question is included in the table which gives the user additional information when prioritizing work. A lower SAL usually means that the fix will be relatively simple. However, while more time consuming and

costly to fix, a higher SAL, represents a higher level of protection. Resources should be allocated according to the calculated rank and the risk tolerance of the user.

Question Comments/Marked for Review: This section includes all the questions that had comments entered or had the Marked for Review check box clicked. It identifies the question by subject area and by number within the subject area and then displays the question, its answer, and the comment.

Alternate Justifications: This table is similar to the question comments table described above except that it provides the text that was entered as a justification for using an alternate method to accomplish the intent of the question.

Site Detail Report

The Site Detail Report adds several new sections to the report that are not found in the Executive Summary or Site Summary Reports.

The following sections have been described in either the [Executive Summary Report](#) or the [Site Summary Report](#) help sections and will not be repeated here. To review the detailed description, please see the respective help section.

- Title Page;
- Disclaimer, Advisory, and Table of Contents;
- Assessment Information;
- Description and Summary;
- Standards Summary;
- Standards Compliance;
- Network Diagram;
- Security Assurance Level (SAL);
- Document Library;
- Ranked Subject Areas;
- Summary of Ranked Questions;
- Question Comments/Marked for Review; and
- Alternate Justifications.

The new section added to the Site Detail Report is a list of the questions detail for each Standard.

Question Details: The final section of the report shows a full list of the questions that were asked and the answers that were given for the Standards. It identifies the question by subject area and by number within the subject area and then displays the question and its answer.

The questions are ordered based on the Standard or the Universal Set and are not ordered by ranking.

Site Cyber Security Plan

The Site Cyber Security Plan provides an overview of the security requirements of the system and describes the controls in place or planned, for meeting those requirements. The Security Plan Report is presented in template format with some generic text (distinguished by being in 10 point font and italicized) that must be replaced with verbiage describing the actual site or facility and the assessment results. Sections to replace include:

- Signature Identification,
- Introduction,
- System identification,
- Roles and Responsibilities, and
- Risk Analysis.

Network Diagram, Zone List, and Inventory List: The report presents a copy of the network diagram scaled to fit on the letter-sized (8.5" × 11") page. It includes a list of the zones that are included in the network diagram if any were identified. The zone information includes the zone name, owner, security level, and the percent implemented. The percent implemented is the number of yes answers per the total number of questions for components in the zone. The report then provides an inventory of all network components that were included in the diagram grouped by zone.

Security Assurance Level (SAL): The SAL page displays the results of the answers and selections related to the SAL. When Cybersecurity Framework is selected as the Assessment Mode, this section will be changed to display the Cybersecurity Framework Tier Determination.

Security Plan Controls and Status List: This section lists all the requirements and controls selected during the assessment. The table includes the requirement title, the control description, affected zones and components, if there are any, and the related questions with the answers that were provided during the assessment. A brief description of each field is provided at the start of the section and repeated below.

Requirement Title: Is the control title as it is generally defined in the Standard document from which this control is derived.

CSET Question/Requirement Category: Shows the CSET Question category from the global questions list. Questions from multiple Standards have been consolidated together in the CSET tool and assigned a common category.

Control Level: Mapped to one of Low, Moderate, High, or Very High.

Implementation Status: Shows the percentage complete as the number of yes answers divided by the total related questions for this control. This percentage implemented will not necessarily be reflective of the amount of work required to implement the control but is merely an indicator of how many of the questions related to the control have been addressed so far.

Short Standard Name: Is an indicator of which Standard this control is derived.

Control Description: The full control text as defined in the Standard from which the control is derived.

Affected Zones: Only applicable to controls derived from a diagram. If a diagram was included in the original assessment, this field will contain a list of zones in which at least one component was found to require this control.

Affected Components: This field contains a list of the components that are directly applicable to this control.

Related Questions and Answers: A list of the questions and answers from which the implementation status of this control was determined.

The table is grouped by control, meaning that there may be several questions under each requirement. The table also summarizes the implementation status of each requirement as a percentage of positive answers per number of related questions. It is ordered to match the on-screen display of the control questions so the user can more easily find and review requirements of interest.

This is the heart of the report. Using this table, the reader can quickly see all the requirements related to the facility and how closely each is being met.

Cybersecurity Framework

When Cybersecurity Framework is selected as the Assessment Mode, the Security Plan Controls and Status List section will change to show information relevant to the Framework. The sections of the table will become as follows.

Framework Function: The high-level framework function indicating in which section of the framework the current control is defined.

Control Category: Shows the framework category from the global questions list.

Implementation Status: Same as described above.

Control Description: The full control text or subcategory as defined in the framework. They are the requirements or required actions.

Observation Tear Out Sheets

Observation records are identified and associated with individual questions during the assessment. As infrastructure or processes are evaluated during the assessment process, there are times when problems or issues are identified. These problems can be recorded and associated with the question under review. The Observation Tear Out Sheets contain a list of all observation records identified during the assessment. The report is formatted such that each observation can be assigned to a person responsible for its resolution and easily assigned.

The Observation Tear Out Sheets report has a fixed set of sections that are all generated when the report is created. Each of the sections in the report will be discussed below.

Title Page: All reports have a cover page that is unique to the report type. The title page includes the assessment name taken from the Information screen in the tool, the date entered in the Assessment Date field, and the name of the person that was entered in the Principal Assessor on the Information screen.

Disclaimer: For information about the Disclaimer, see the [Disclaimer](#) help section.

Advisory: For information about the Advisory, see the [Advisory](#) help section.

Table of Contents: This is a system-generated table that indicates the report sections and the page numbers for those sections.

Site Information: This section displays the text entered on the Information screen in the CSET tool. It displays all entered data with the appropriate labels.

For more information about Site Information, see the [Site Information Screen](#) help section.

Discovery List: Provides a list of all observations identified during the assessment along with the question associated to the observation.

For more information about observation records, see the [Observations Section](#) help section.

Submit Feedback

You can use the Submit Feedback section to view/send all comments entered in the feedback field in the Assessment screen. You can either copy the text of the populated message and edit and send at your discretion or use the email button to select your email client and edit and send from there.

Note: The Submit Feedback tab doesn't allow for editing the feedback added during the assessment. Feedback needs to be edited from the assessment. All feedback from any assessment will be shown in the Feedback screen. Not just the feedback from the active assessment.

The screenshot shows the CSET software interface. At the top, there is a navigation bar with the CSET logo, a 'Tools' dropdown, a 'Resource Library' link, a 'Help' link, and a 'Your Username' dropdown. Below the navigation bar, there is a horizontal menu with tabs: 'Prepare', 'Diagram', 'Questions', and 'Results'. The 'Results' tab is currently selected and highlighted in blue. On the left side, there is a sidebar with several sections and links: 'Analysis Dashboard', 'Control Priorities', 'Standards Summary', 'Ranked Categories', 'Results by Category', 'Components Summary', 'Ranked Categories', 'Results by Category', 'Component Types', 'Network Warnings', 'Executive Summary, Overview, & Comments', 'Reports', and 'Submit Feedback'. The main content area is titled 'Submit Feedback to DHS'. It contains instructions: 'Please ensure that the feedback you provide does not include any proprietary or assessment related information. These comments should be considered part of a public community discussion with regard to the FAA PED module'. Below this, there is a text input field with placeholder text: 'Copy text to clipboard and paste into an email'. There are two buttons below the input field: 'CopyText' and 'Email'. To the right of the input field, there is a text area labeled 'Please email to:' containing the email address 'cset@dhs.gov'. Below this, there is a text area labeled 'Dear PED Module Administrator:' followed by a message: 'The following comments were provided for each of the questions: Users Feedback: THIS is feedback'. At the bottom of the main content area, there is a question: 'Are appropriate agreements finalized before access is granted, including for third parties and contractors?'. A vertical scroll bar is visible on the right side of the main content area.

Figure: Submit Feedback screen

Initiation Scenarios

The following initiation scenarios are provided as an overview of typical security vulnerabilities associated with shared control system and business system infrastructure or control systems connected to other external networks (hereafter any non-control system is referred to as an external network). It is intended that this information will stimulate thought and discussion for the team performing a CSET assessment, specifically, in determining a SAL. This overview is not intended to be a comprehensive review of all potential threats or vulnerabilities.

Three aspects must be considered when assessing the security posture of a control system:

Availability. The system must be ready and able to store and transmit data when needed.

Integrity. The data stored or transmitted by the system must be complete and correct (not corrupted).

Confidentiality. The system must be able to store and transmit data without unauthorized disclosure of sensitive information.

The following pages describe a typical ICS/external network environment and provide examples of risks, exposures, and vulnerabilities that are commonly encountered in such environments.

Typical Mixed-Use Control/External Network Environment

In a typical mixed-use environment, there is separation between ICSs and external networks, but both rely on some amount of shared infrastructure (e.g., communications links). Although separated, some connectivity between these networks exists (e.g., public web or application servers).

There are typically distinct but interconnected networks, including the following:

Control System. The control system consists of servers, workstations, and devices associated with the ICSs. Multiple separate systems may be in use and individual systems may span multiple sites.

Business Network. The business network consists of servers and workstations associated with typical office productivity applications, such as email and word processing, as well as specialized applications such as for human resources, payroll, and billing.

Other Networks. These consist of other city, state, federal, or outside agency networks connected via dedicated communications, Virtual Private Networks (VPNs), or other means. Typically, access from such networks is controlled via a firewall. Connections to other networks may be trusted or untrusted.

Internet. For the public Internet, typically, access is allowed to the outside for business use (e.g., email, web browsing) and limited services may be accessed externally (e.g., web access to public information). Such access is controlled via a firewall, and the Internet is treated as an untrusted network.

Shared Infrastructure. While the ICS and business environments are distinct, there are touch points between them.

Because of the costs and complexity associated with wide area networks, it is common to allow both ICS and normal business communications to share the same physical infrastructure.

The need to share information may drive the use of portals between networks in a dual-homed configuration with direct connection to both networks, or shared servers may be placed on a DMZ network between the ICS and the business.

ICS personnel with the need for business application access may be provided workstations that are dual-homed or provided access to the business network from their ICS workstations, or vice versa.

It is important to appreciate the complexity of ensuring security in such environments.

While individual products, systems, or networks may be secure when taken individually, they may not be adequately secured or protected in a complex deployment.

Common Initiation Scenarios

The following scenarios describe common security issues that can initiate a worst-case scenario. The scenarios could impact the operation of a facility causing damage, loss of production, impacts to health, safety, and the environment, or other economic impacts. These issues could, in turn, impact system availability, integrity, and confidentiality in a typical mixed-use environment. These scenarios are provided as food for thought in developing an organization's worst-case scenario and the resulting consequences.

Scenario 1: Privilege Escalation

In this scenario, an unknown party (attacker) is able to access sensitive data or systems by means of existing network connections. This access may be gained by a number of means, including:

Insufficiently Protected Networks. Restrictions between networks may be nonexistent, poorly implemented, or may rely on excessive levels of trust between networks.

Privilege Escalation. The outsider, or in some cases an insider, may access a public or loosely secured system with limited functionality and then use that system to hop to more sensitive functions. By hopping between systems, the attacker appears to be operating from inside the trusted network.

Poorly Secured Resources. A determined attacker can potentially exploit a number of system weaknesses, including but certainly not limited to the following:

- Unsecured Default Accounts. The attacker leverages widely known default accounts and passwords to gain access.
- Poorly Secured Services. The attacker uses weaknesses in running services and applications to gain access to increased access levels (i.e., gaining access to sensitive system files).
- Weak Network Services. The attacker uses known vulnerabilities in services and applications to execute programs to gain further levels of access.

The attacker might proceed as follows:

- 1) Identifying the software running on the web server. While doing simple Internet searches, the attacker locates software capable of exploiting vulnerabilities within the web server software or the current configuration of the server to allow execution of programs on the web server.
- 2) Executing a remote shell (command prompt) on the web server to launch software identifying internal hosts. Upon discovery of an interesting server (the Control System Historian in this example), the attacker attempts to gain access using well-known default accounts (i.e., Guest), eventually discovering a little-used account with a default, or easily guessed password to gain access.
- 3) Using the trust associated with the control system Historian to gain access to the ICS network. In poorly secured systems, there may be excessive trust between inside servers and the ICS, which can allow easy access. Once in, the attacker uses additional probes to gain access to ICSs and to install software, view and manipulate data, or perform any other desired function.

Any such intrusion impacts the ICS network at multiple levels:

Availability. Through intentional or accidental reconfiguration, the attacker may disable essential system services, or introduce software (i.e., spam generators) that disrupts the network because of the traffic loads generated.

Integrity. Unauthorized manipulation of data can be done at the attacker's whim. This may range from simple curious tinkering to direct attempts to impact the ICS.

Confidentiality. Sensitive system functions may be identified, and data may be accessed and disseminated to unknown third parties.

Scenario 2: Traffic Sniffing

In this scenario, shared network infrastructure (e.g., hubs, switches, routers) is used for both the ICS and business. An unauthorized user (attacker) on a non-ICS network is able to sniff network traffic and capture login credentials (username, password), sensitive data, and network information.

The attacker might proceed as follows:

- 1) In a direct attempt to sabotage the ICS, or simply out of curiosity, the attacker installs packet capture (sniffer) software to monitor traffic on the network. This software is capable of capturing any visible traffic and may include the means to circumvent protection offered by switches. In an extreme case, the attacker can use man-in-the-middle attacks to circumvent encryption. Such software can be monitored in real time or simply run in the background to capture traffic of interest. In particular, user login IDs and passwords can be captured in this manner.
- 2) An authorized user eventually connects to the ICS using authentication credentials (username and password). Because of weaknesses in the application, the password is not encrypted or is encrypted using weak and easily circumvented techniques.
- 3) Having captured the login session, the attacker simply extracts the password from the network traffic stream (if clear text) or runs a password-cracking program against it (if encrypted). Once the user account details are known, the attacker is free to impersonate that user and gain access to the ICS.

Any such attack impacts the ICS network at multiple levels:

Availability. The attacker may intentionally or inadvertently disable the user account. Changes to device configurations may result in a loss of use.

Integrity. With access into the system, the attacker can make further attempts to use the same credentials on other systems. Unauthorized manipulation of data can be done at the attacker's whim. This may range from simple curious tinkering to directed attempts to impact the ICS.

Confidentiality. Once user credentials are compromised, the attacker may impersonate the user at will. Sensitive system functions may be identified, and data may be accessed and disseminated to unknown third parties.

Scenario 3: Introduction of Malicious Software from Outside the System

In this scenario, a workstation used by an authorized user is compromised by means of malicious software, or malware such as Trojan horses, viruses, or worms (in any combination). Such software is typically written to allow the attacker to generate spam emails.

The sequence of events might occur as follows:

1) A user on an operator workstation with either connections into both networks (dual-homed) or an internal ICS workstation with access to the outside inadvertently downloads a program via an email attachment. Although most users know not to run programs from unknown outsiders, simple carelessness or a well-crafted social engineering message appearing to come from Network Support might convince them to launch the attached program. The program exploits vulnerability in the workstation operating system to install malware (a worm). Once installed, the worm begins replication thus filling the memory.

2) Eventually, the sheer volume of traffic generated by multiple copies of the worm running on the network overwhelms lower-speed Wide Area Network (WAN) links, resulting in loss of communications or a denial of service.

Any such attack impacts the ICS network at multiple levels, such as:

Availability. The most likely impact is network disruption due to the sheer volume of worm-related traffic (e.g., probes, spam, and bounce email messages.)

Integrity. Remote-control software allows the attacker unrestricted access to the compromised system. If the attacker has some means of accessing the system, unauthorized manipulation of data can be done at the attacker's whim. This may range from simple curious tinkering to directed attempts to impact the ICS.

Confidentiality. If remote-control software is installed, sensitive system functions may be identified and data accessed and disseminated to unknown third parties.

Glossary

Acronyms

Acronym	Definition
ALT	Alternate Method
C2M2	Cybersecurity Capability Maturity Model
CAG	Consensus Audit Guidelines
CCI	Control Correlation Identifier
CFATS	Chemical Facility Anti-Terrorism Standards
CFR	Code of Federal Regulations
CIP	Critical Infrastructure Protection
CIS	Center for Internet Security
CMMS	• Computerized Maintenance Management System
CNSSI	Committee on National Security Systems Instruction
CoR	Catalog of Recommendations
CSET	Cyber Security Evaluation Tool
CUI	Controlled Unclassified Information
DCS	Distributed Control System
DHS	U. S. Department of Homeland Security
DISA	Defense Information Systems Agency
DoD	U. S. Department of Defense
eMASS	Enterprise Mission Assurance Support Service
FIPS	Federal Information Processing Standards
HIPAA	Health Insurance Portability and Accountability Act of 1996
HMI	Human-Machine Interface
ICS	Industrial Control System
ICT	Information and Communications Technology
IDS	Intrusion Detection System
IIS	Internet Information Services
INGAA	Interstate Natural Gas Association of America
IR	Interagency Report
IT	Information Technology
MAC	Mission Assurance Category
MIL	Maturity Indicator Level
MSC	Multiple Services Component
NA	Not Applicable
NEI	Nuclear Energy Institute
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
PCIDSS	Payment Card Industry Data Security Standard
PDF	Portable Document Format
PII	Personally Identifiable Information
PLC	Programmable Logic Controller
RBPS	Risk-Based Performance Standards

RG	Regulatory Guidelines
SAL	Security Assurance Level
SCADA	Supervisory Control and Data Acquisition
SP800	Special Publication 800
TSA	Transportation Security Administration
URL	Uniform Resource Locator
USB	Universal Serial Bus
VPN	Virtual Private Network

Key Terms

Term	Explanation
Admin Questions	Questions spawned by the tool in response to the applied Standards the user selects.
Assessment Documents	Repository of documents added to the assessment by the user.
Assessment Report	A summary report of results for each question including user responses, statement of actual requirements (or deficiencies), answers in relation to the overall SAL, and associated help documents.
Classified Information	Any information or material that has been determined by the U.S. Government pursuant to an executive order, statute, or regulation, to require protection against unauthorized disclosure for reasons of national security (Classified Information Procedures Act, 18 U.S. Code App. 3, Section 1(a)).
Component Diagram or Network Diagram	A network topology that best represents the industrial control system configuration. Diagram includes typical components associated with a control system such as connector, firewall, network router, network switch, serial switch, network hub, modem, programmable logic controller, remote terminal unit, HMI, engineering workstation, intrusion detection system, wireless access point, serial radio, application server, database server, terminal server, web server, virtual private network, link encryption, DCS, printer, and clock.
Component Questions	A generated list of control system cybersecurity questions based on the defined SAL and components contained within the network topology diagram.
Confidentiality Level	Applicable to DoD information systems, the confidentiality level is primarily used to establish acceptable access factors, such as requirements for individual security clearances or background investigations, access approvals, and need-to-know determinations; interconnection controls and approvals; and acceptable methods by which users may access the system (e.g., intranet, Internet, wireless). The DoD has three defined confidentiality levels: classified, sensitive, and public.
Critical Asset	Those facilities, systems, and equipment, which if destroyed, damaged, degraded, or otherwise rendered unavailable, would have a significant impact on the ability to serve large quantities of customers for an extended period of time, would have a detrimental impact on the reliability or operability of the electric grid, or would cause significant risk to public health and safety.
Mission Assurance Category	Applicable to DoD information systems, the mission assurance category reflects the importance of information relative to the achievement of DoD goals and objectives. Mission assurance categories are primarily used to determine the requirements for availability and integrity. The DoD has three defined mission assurance categories: MAC I, MAC II, and MAC III. MAC I systems require the most stringent protection measures.

Public Information	Official information that has been reviewed and approved for public release by the information owner.
Resource Library	Electronic copies of cybersecurity documentation are included in the tool for reference, including federal codes, white papers, reports, industry Standards, and guidelines.
Security Assurance Level	<p>The relative consequences of a successful attack against the control system being evaluated. The consequence analysis identifies the worst, reasonable consequence that could be generated by a specific threat scenario. The General SAL provides an overall rating of the criticality based on the users' review of security threat scenarios and estimated consequences.</p> <p>The SAL ranges from Low to Very High.</p>
Security Categories	<p>The security categories are related to the NIST 800-53 Standards and are defined as:</p> <p>CONFIDENTIALITY “Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information...” A loss of confidentiality is the unauthorized disclosure of information.</p> <p>INTEGRITY “Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity...” A loss of integrity is the unauthorized modification or destruction of information.</p> <p>AVAILABILITY “Ensuring timely and reliable access to and use of information...” A loss of availability is the disruption of access to or use of information or an information system.</p>
Security Categorization	<p>The NIST 800-53-related security categorizations of Low, Moderate, and High are explained as:</p> <p>LOW: The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.</p> <p>AMPLIFICATION: A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.</p> <p>MODERATE: The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.</p> <p>AMPLIFICATION: A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.</p> <p>HIGH: The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.</p>

	AMPLIFICATION: A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.
Security Level	The rating of High, Moderate, or Low for Confidentiality, Integrity, and Availability according to FIPS 199 and NIST SP800-60.
Sensitive Information	Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an executive order or an act of Congress to be kept secret in the interest of national defense or foreign policy.

Frequently Asked Questions (FAQs)

This is a list of questions that new users may find helpful.

My system is running slow. How can I make it go faster?

This release may run slower than previous releases of CSET. Check to make sure that there is sufficient RAM on the user's computer. 3 GB of RAM is recommended. Check the Task Manager to verify that the computer is not paging to the disk drive, which would cause a significant drop in performance. The delays typically come from the system loading and caching data between the main screens. There is a greater delay when using a large diagram or when multiple Standards are selected. A faster processor will also help.

How do I import a file from a previous release of CSET?

See [Import a CSET Assessment](#) for more information.

Why isn't the Catalog of Recommendations available in Questions mode on the Standards screen?

The Catalog of Recommendations, Version 7 was the foundation for the Universal Questions and so to select it would be to double-select the same set of questions. To avoid confusion, it is not selectable in Questions mode.

What Standard should I use?

Only the user can answer that question for his or her organization; however, extensive help information can be found by reviewing the [Cybersecurity Standard Selection](#) help section. The user may also consult the User Guide available from the home screen. For a brief description of the available Standards, see the [CSET Standards and Question Groupings](#) help section.

Can I unclick an answer in the Questions screen after making a selection?

Yes. Simply click the button again to clear it.

I've lost my zone on the diagram. Where did it go?

Like other shapes, it may have been placed behind another zone or another shape. You can move or minimize the shapes to see if it is hidden behind them. You can also go to the Format tab and use the options found under the Commands menu to move zones and other shapes forward and backward in the view order. To quickly see what is behind a zone or shape, send it to the back.

You might also check to see if it has been assigned to a layer that is not displayed. Click the Home tab and select Layers. Make sure all layers are checked.

I put in a text box on the diagram and want to change the style. How do I do it?

Text objects are placed onto the diagram while in the Format menu tab. The formatting can be found under the same tab or by clicking the gear icon to open the properties popup box. Go to Format, click on the text block, and make the changes using the Label Styles commands. You can change font, size, bold, italic, underline, color, and position.

I'm having trouble connecting components on the diagram. Is there a trick to it?

This can be a bit tricky, especially when there are multiple lines. First, click the Selector tool under the Format tab. Then, select the starting component. This will put a gray box around it. Click inside the gray border and hold the mouse down to drag the line to the second component. Hover over the center of the second component until the link area turns red, then click. The problem comes if you click that spot again to draw another line. The system may think you are trying to move the first line, not start a new one. Click outside of the component to finalize the first line before starting another from the same point.

I'm in the diagram and can't seem to change modes. How do I know where I am and how do I change?

The selected mode or function is identified by a blue background on the icon. This could remain active even if you change menu options by selecting a new tab. Clicking on a different function will change the mode. For example, to stop creating text boxes, click on the Selector tool under the Format menu. There are cases where a function will remain active even with a new button clicked. For example, Analyze Network is a toggle switch that is independent of other actions.

Can I change properties on multiple objects at once?

Yes, you can select multiple objects; however, the only property that can be changed for all of them is the Layer. You can also use the multi-select to remove the unique flag and remove the question overrides, if there are any. To select multiple objects, you can drag a box around them with the Selector tool enabled in the Format tab. Unfortunately, this can often capture nearby, but unwanted, objects. Another method is to hold down the keyboard Control (Ctrl) key while clicking the desired objects with the mouse.

I have a Microsoft Visio diagram. Can I use it?

No, not with the current version of CSET. This will be a future option.

In the Components Summary Screen the number of Questions doesn't seem to add up. What is happening?

There may be a situation where you have two components of the same type and see an odd number of questions in the analysis screen. This would occur if the components are in zones with different security assurance levels (SALs). For example, an application server in a zone with a low SAL may have 10 associated questions and an application server in a zone with a high SAL may have 15 questions associated with it, due to the higher requirements. The total number of questions would be 25 for both servers.

CSET Revision History

Document Revision	Date	Change Description
0	August 2009	Initial release
1.0	April 2010	Updated Regulatory Basis in Section 2. Added instructions for new functionality in the drawing tool.
1.1	May 2010	Added need for Word 2007 to support RTF report. Revised description of component diagram zones.
2.0	August 2010	Updated Regulatory Basis in Section 2. Added instructions for new navigation and user interface.
3.0	July 2011	Updated Regulatory Basis in Section 2. Added instructions for the resource library, diagram layering, line security, and new report format.
4.0	January 2012	Updated the component diagram section to explain the use of Microsoft Visio.
5.0	December 2012	New architectural change to .NET and new approach with questions and requirements. New diagramming tool and system redesign for ease of use. Added new standards and modified default approach for component questions. Added new analysis capabilities and enhance resource library.
5.1	June 2013	Modifications to the Questions screen with headings, new standards, and modifications to standards and analysis to accommodate the CNSSI baseline and overlay.
6.0	January 2014	Added aggregation functionality and new standards, modified the diagram interface to improve usability, added the ability to create a component inventory list from the diagram, and added new Security Plan Report option. Video tutorials were moved to YouTube for online viewing.
6.1	July 2014	Added new Cybersecurity Framework mode to the standards options, revised the Analysis function to include Framework details, and modified the Network Diagram tool to improve how Zones are used and to clarify tab and menu names.
6.2	January 2015	Added fields for the Real Property and Site Unique Identification (RDSUID) information, added a new Security Assurance Level (SAL) determination for CNSS, added functionality to import information pertaining to the network diagram from Grass Marlin, added functionality to export information pertaining to eMASS, and added two new standards.
7.0	August 2015	Implemented a new, more modern design for the tool. Increased responsiveness of the Questions and Diagram screens. Added Cybersecurity Capability Maturity Model (C2M2), DoD Instruction 8510.01, and NISTIR 7628 Volume 1, Revision 1 as new standards.
7.1	January 2016	Added 43 new components to the diagram including new radio and medical components. Added ability to change parameter values on requirement text. Redesigned the analysis screens and added NERC Rev. 5 Compliance analysis capability. Added NIST SP800-161 Supply Chain Risk Management. Deprecated CNSSI 1253 Baseline and Overlay Standards.
8.0	September 2016	Redesigned the overall process to streamline the Preparation, Assessment, and Results processes and make the CSET tool easier to use by novice users. Added the ability to create custom questionnaires or custom question sets from any of the existing

standard questions. Added the following Standards: Control Correlation Identifier Specification V2 Release 0.1, Critical Security Controls Version 6, Health Insurance Portability and Accountability Act Security Rule and NIST Special Publication 800-171. Added ability to collect discoveries on questions. Added four new components/symbols to the diagram.

8.1	February 2018	Fixed several application errors and started adding basic accessibility functionality to address 508 requirements.
9.0	October 2018	Moved to a web application with mobile capabilities.
9.0.1	April 2019	Added Module Builder for creating custom question/requirement sets. Added standard NIST 800-53 R5.
9.2.0	November 2019	Added Diagram capability. Added the TSA Pipeline March 2018 and ISA-62443-4-1-2018 standards.
9.2.1	November 2019	Bug Release.