

UNCLASSIFIED



AvePoint Fly Server Security Technical Implementation Guide

Version: 1

Release: 1

28 Apr 2026

XSL Release 1/25/2022 Sort by: STIGID

Description: This Security Technical Implementation Guide is published as a tool to improve the security of Department of War (DoW) information systems. The requirements are derived from the National Institute of Standards and Technology (NIST) 800-53 and related documents. Comments or proposed revisions to this document should be sent via email to the following address: disa.stig_spt@mail.mil.

Group ID (Vulid): V-283924

Group Title: SRG-APP-000001

Rule ID: SV-283924r1206887_rule

Severity: CAT II

Rule Version (STIG-ID): [FLYS-00-000005](#)

Rule Title: Fly Server must limit the number of concurrent sessions for all accounts and/or account types.

Vulnerability Discussion: Application management includes the ability to control the number of users and user sessions that use an application. Limiting the number of allowed users and sessions per user is helpful in limiting risks related to denial-of-service (DoS) attacks.

This requirement may be met via the application or by using information system session control provided by a web server with specialized session management capabilities. If it has been specified that this requirement will be handled by the application, the capability to limit the maximum number of concurrent single user sessions must be designed and built into the application.

This requirement addresses concurrent sessions for information system accounts and does not address concurrent sessions by single users via multiple system accounts. The maximum number of concurrent sessions must be defined based upon mission needs and the operational environment for each system.

Check Content:

Check the Fly Server Manager session setting:

- Log on to Fly Server Manager with an admin account.
- On the Management >> General Settings page, click the "System Option" tab.
- Verify the "Allow concurrent sessions from multiple servers for the same account" setting.

If this setting is checked, this is a finding.

Fix Text: Configure the Fly Server Manager session setting:

- Log on to Fly Server Manager with an admin account.
- On the Management >> General Settings page, click the "System Option" tab.
- Uncheck the "Allow concurrent sessions from multiple servers for the same account" setting.
- Save the setting.

CCI: CCI-000054

Group ID (Vulid): V-283925

Group Title: SRG-APP-000025

Rule ID: SV-283925r1206871_rule

Severity: CAT II

Rule Version (STIG-ID): [FLYS-00-000015](#)

Rule Title: Fly Server must automatically disable accounts after a 35-day period of account inactivity.

Vulnerability Discussion: Attackers that are able to exploit an inactive account can potentially obtain and maintain undetected access to an application. Owners of inactive accounts will not notice if unauthorized access to their user account has been obtained. Applications need to track periods of user inactivity and disable accounts after 35 days of inactivity. Such a process greatly reduces the risk that accounts will be hijacked, leading to a data compromise.

To address access requirements, many application developers choose to integrate their applications with enterprise-level authentication/access mechanisms that meet or exceed access control policy requirements. Such integration allows the application developer to off-load those access control functions and focus on core application features and functionality.

This policy does not apply to either emergency accounts or infrequently used accounts. Infrequently used accounts are local login administrator accounts used by system administrators when network or normal logon/access is not available. Emergency accounts are administrator accounts created in response to crisis

situations.

Check Content:

Check the Fly Server security settings:

- Log on to Fly Server Manager with the admin account.
- On the Management >> General Settings page, click the "Security Option" tab.
- Navigate to "User Settings".
- Verify the "Deactivate a user after 35 days of inactivity" option is checked.

If this option is not checked, this is a finding.

Fix Text: Configure the Fly Server security settings:

- Log on to Fly Server Manager with the administrator account.
- On the Management >> General Settings page, click the "Security Option" tab.
- Navigate to "User Settings", then click "Deactivate a user after 35 days of inactivity" option.
- Set 35 days or other values as required.
- Save the setting.

CCI: CCI-000017

Group ID (Vulid): V-283926

Group Title: SRG-APP-000065

Rule ID: SV-283926r1206132_rule

Severity: CAT II

Rule Version (STIG-ID): [FLYS-00-000020](#)

Rule Title: Fly Server must enforce the limit of three consecutive invalid logon attempts by a user during a 15 minute time period.

Vulnerability Discussion: By limiting the number of failed login attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute forcing, is reduced. Limits are imposed by locking the account.

Satisfies: SRG-APP-000065, SRG-APP-000345, SRG-APP-000295, SRG-APP-000317

Check Content:

Check the logon configuration in Fly Server Manager:

- Access the VM or server where the Fly Server manager is installed.
- Find the installation location of Fly Server manager.
- Open the "TimerService.exe.config" file in ...\\APElements\\FLY\\Manager\\Control\\bin.
- Check the key "FailedLogOnLimitationCount".

If the value is not "3", this is a finding.

Fix Text: Configure the logon configuration in Fly Server Manager:

- Access the VM or server where the Fly Server manager is installed.
- Find the installation location of Fly Server manager.
- Open the "TimerService.exe.config" file in ...\\APElements\\FLY\\Manager\\Control\\bin.
- Find following node and set the value to "3":

```
<add key="FailedLogOnLimitationCount" value="3" />
```

CCI: CCI-000044

CCI: CCI-002238

CCI: CCI-002361

CCI: CCI-004045

Group ID (Vulid): V-283927

Group Title: SRG-APP-000142

Rule ID: SV-283927r1206911_rule

Severity: CAT II

Rule Version (STIG-ID): [FLYS-00-000035](#)

Rule Title: Fly Server must be configured to prohibit or restrict the use of organization-defined functions, ports, protocols, and/or services, as defined in the Ports, Protocols, and Services Management Category Assurance List (PPSM CAL) and vulnerability assessments.

Vulnerability Discussion: Authenticity protection provides protection against man-in-the-middle attacks/session hijacking and the insertion of false information into sessions.

Application communication sessions are protected using transport encryption protocols, such as TLS, which provides web applications with a means to be able to authenticate user sessions and encrypt application traffic. Session authentication can be single (one-way) or mutual (two-way) in nature. Single authentication authenticates the server for the client, whereas mutual authentication provides a means for both the client and the server to authenticate each other.

This requirement applies to applications that use communications sessions. This includes, but is not limited to, web-based applications and service-oriented architectures (SOAs).

This requirement addresses communications protection at the application session, versus the network packet, and establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted. Depending on the required degree of confidentiality and integrity, web services/SOA will require the use of TLS mutual authentication (two-way/bidirectional).

Check Content:

Open the Fly Server console in a browser and note the port number in the URL.

Fly Server uses ports 20100 and 20101 by default for Manager and Agent internal communication.

If the ports used are organization-defined to be in use by another system, this is a finding.

Fix Text: Configure the internal communication ports for Fly Server Manager and Agent.

- Install Fly Server Manager and Agent.
- Set Manager Access URL and Internal Communication Port setting, set to ports that are not organization-defined to be in use by another system.

CCI: CCI-000382

Group ID (Vulid): V-283928

Group Title: SRG-APP-000155

Rule ID: SV-283928r1223356_rule

Severity: CAT I

Rule Version (STIG-ID): FLYS-00-000055

Rule Title: Fly Server must use an approved DoW enterprise identity, credential, and access management (ICAM) solution to uniquely identify and authenticate organizational users.

Vulnerability Discussion: To ensure accountability and prevent unauthenticated access, organizational users must be identified and authenticated to prevent potential misuse and compromise of the system. This is typically accomplished via the use of a user store, which is either local (OS-based) or centralized (LDAP) in nature. However, DODI 8520.03 now requires that applications use an approved DoW enterprise (E-ICAM) solution whenever the ICAM solution addresses information system needs. Where the ICAM solution has been evaluated and found to not meet the needs of information system owners, information system owners must reevaluate decisions to use locally managed solutions and transition to DoW enterprise ICAM solutions to the maximum extent possible as the enterprise ICAM solutions mature.

Satisfies: SRG-APP-000155, SRG-APP-000023, SRG-APP-000149, SRG-APP-000150, SRG-APP-000154, SRG-APP-000156, SRG-APP-000174, SRG-APP-000318, SRG-APP-000334, SRG-APP-000391, SRG-APP-000392, SRG-APP-000402, SRG-APP-000403, SRG-APP-000404, SRG-APP-000405, SRG-APP-000461, SRG-APP-000700, SRG-APP-000705, SRG-APP-000710, SRG-APP-000740, SRG-APP-000820, SRG-APP-000825, SRG-APP-000830, SRG-APP-000875, SRG-APP-000960, SRG-APP-000965, SRG-APP-000970, SRG-APP-000975, SRG-APP-000980, SRG-APP-000985, SRG-APP-000990, SRG-APP-000995, SRG-APP-001000, SRG-APP-000148, SRG-APP-000153, SRG-APP-000157, SRG-APP-000212, SRG-APP-000389, SRG-APP-000175, SRG-APP-000176, SRG-APP-000177, SRG-APP-000395, SRG-APP-000400, SRG-APP-000401, SRG-APP-001005, SRG-APP-001010, SRG-APP-001015, SRG-APP-001020, SRG-APP-001025

Check Content:

Fly Server must be integrated with Active Directory (AD) and Azure AD (AAD) for automated account management.

Check the Fly Server Account Manager setting to verify AD Integration or AAD Integration is enabled:

- Log on to Fly Server with an admin account.
- On the Management >> Account Manager page, click "Authentication Manager".
- Navigate to AD Integration or AAD Integration.
- Verify the AD Integration or AAD Integration option is enabled.

If the AD Integration or AAD Integration option is not enabled, this is a finding.

Fix Text: Configure the Fly Server Account Manager setting to ensure AD Integration or AAD Integration is enabled:

- Log on to Fly Server with an admin account.
- On the Management >> Account Manager page, click "Authentication Manager".
- Navigate to AD Integration or AAD Integration.
- Set the Action of AD Integration or AAD Integration to "Enable".
- Add an AD domain after AD integration is enabled.
- Save the setting.

Add AD user/group or AAD user/group to Account Manager; realize automated mechanisms through AD or AAD account management functions.

CCI: CCI-004046

CCI: CCI-000015

CCI: CCI-000765

CCI: CCI-000766

CCI: CCI-001941

CCI: CCI-004066

CCI: CCI-002145

CCI: CCI-002205

CCI: CCI-000366

CCI: CCI-001953

CCI: CCI-001954

CCI: CCI-002009

CCI: CCI-002010

CCI: CCI-004083

CCI: CCI-004085

CCI: CCI-003747

CCI: CCI-003627

CCI: CCI-003628

CCI: CCI-003629

CCI: CCI-004047

CCI: CCI-004058

CCI: CCI-004068

CCI: CCI-005155

CCI: CCI-005156

CCI: CCI-005157

CCI: CCI-005158

CCI: CCI-005159

CCI: CCI-005160

CCI: CCI-005161

CCI: CCI-005162

CCI: CCI-005163

CCI: CCI-000764

CCI: CCI-004045

CCI: CCI-001083

CCI: CCI-002038

CCI: CCI-000185

CCI: CCI-000186

CCI: CCI-000187

CCI: CCI-001967

CCI: CCI-002007

CCI: CCI-005164

CCI: CCI-005165

CCI: CCI-005166

CCI: CCI-005167

CCI: CCI-005168

Group ID (Vulid): V-283929

Group Title: SRG-APP-000164

Rule ID: SV-283929r1206891_rule

Severity: CAT II

Rule Version (STIG-ID): [FLYS-00-000065](#)

Rule Title: Fly Server must enforce a minimum 15-character password length.

Vulnerability Discussion: The shorter the password, the lower the number of possible combinations that need to be tested before the password is compromised.

Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. Password length is one factor of several that helps to determine strength and how long it takes to crack a password. The shorter the password, the lower the number of possible combinations that need to be tested before the password is compromised.

Use of more characters in a password helps to exponentially increase the time and/or resources required to compromise the password.

Check Content:

Fly Server must be integrated with Active Directory (AD) and Azure AD (AAD) for automated account management.

Check the Fly Server Account Manager setting to verify AD Integration or AAD Integration is enabled:

- Log on to Fly Server with an admin account.
- On the Management >> Account Manager page, click "Authentication Manager".
- Navigate to AD Integration or AAD Integration.
- Verify the AD Integration or AAD Integration option is enabled.

If the AD Integration or AAD Integration option is not enabled, this is a finding.

Fix Text: Configure the Fly Server Account Manager setting to ensure AD Integration or AAD Integration is enabled:

- Log on to Fly Server with an admin account.
- On the Management >> Account Manager page, click "Authentication Manager".
- Navigate to AD Integration or AAD Integration.
- Set the Action of AD Integration or AAD Integration to "Enable".
- Add an AD domain after AD integration is enabled.
- Save the setting.

Add AD user/group or AAD user/group to Account Manager; realize automated mechanisms through AD or AAD account management functions.

CCI: CCI-004066

Group ID (Vulid): V-283930

Group Title: SRG-APP-000166

Rule ID: SV-283930r1206893_rule

Severity: CAT II

Rule Version (STIG-ID): [FLYS-00-000070](#)

Rule Title: Fly Server must enforce password complexity by requiring that at least one uppercase character be used.

Vulnerability Discussion: Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determine how long it takes to crack a password. The more complex the password is, the greater the number of possible combinations that need to be tested before the password is compromised.

Check Content:

Check the Fly Server Manager security configuration:

- Log on to Fly Server with an admin account.
- On the Management >> General Settings page, click the "Security Option" tab.
- Verify the Password Complexity setting.

If the Password complexity setting is not set to Custom, with checkboxes enabled for uppercase letters, lowercase letters, numerical digits, and special characters, this is a finding.

Fix Text: Configure the Fly Server Manager security configuration:

- Log on to Fly Server with an admin account.
- On the Management >> General Settings page, click the "Security Option" tab.
- Set the Password Complexity setting to Custom, select four checkboxes to enforce that the password must contain four character types: uppercase letters, lowercase letters, digits, and special characters.

CCI: CCI-004066

Group ID (Vulid): V-283931

Group Title: SRG-APP-000167

Rule ID: SV-283931r1206876_rule

Severity: CAT II

Rule Version (STIG-ID): [FLYS-00-000075](#)

Rule Title: Fly Server must enforce password complexity by requiring that at least one lowercase character be used.

Vulnerability Discussion: Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determine how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Check Content:

Check the Fly Server Manager security configuration:

- Log on to Fly Server with an admin account.
- On the Management >> General Settings page, click the "Security Option" tab.
- Verify the Password Complexity setting.

If the Password complexity setting is not set to Custom, with checkboxes enabled for uppercase letters, lowercase letters, numerical digits, and special characters, this is a finding.

Fix Text: Configure the Fly Server Manager security configuration:

- Log on to Fly Server with an admin account.
- On the Management >> General Settings page, click the "Security Option" tab.
- Set the Password Complexity setting to Custom, select four checkboxes to enforce that the password must contain four character types: uppercase letters, lowercase letters, digits, and special characters.

CCI: CCI-004066

Group ID (Vulid): V-283932

Group Title: SRG-APP-000168

Rule ID: SV-283932r1206878_rule

Severity: CAT II

Rule Version (STIG-ID): [FLYS-00-000080](#)

Rule Title: Fly Server must enforce password complexity by requiring that at least one numeric character be used.

Vulnerability Discussion: Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determine how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Check Content:

Check the Fly Server Manager security configuration:

- Log on to Fly Server with an admin account.
- On the Management >> General Settings page, click the "Security Option" tab.
- Verify the Password Complexity setting.

If the Password complexity setting is not set to Custom, with checkboxes enabled for uppercase letters, lowercase letters, numerical digits, and special characters, this is a finding.

Fix Text: Configure the Fly Server Manager security configuration:

- Log on to Fly Server with an admin account.
- On the Management >> General Settings page, click the "Security Option" tab.
- Set the Password Complexity setting to Custom, select four checkboxes to enforce that the password must contain four character types: uppercase letters, lowercase letters, digits, and special characters.

CCI: CCI-004066

Group ID (Vulid): V-283933

Group Title: SRG-APP-000169

Rule ID: SV-283933r1206880_rule

Severity: CAT II

Rule Version (STIG-ID): [FLYS-00-000085](#)

Rule Title: Fly Server must enforce password complexity by requiring that at least one special character be used.

Vulnerability Discussion: Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor in determining how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Special characters are those characters that are not alphanumeric. Examples include: ~ ! @ # \$ % ^ *.

Check Content:

Check the Fly Server Manager security configuration:

- Log on to Fly Server with an admin account.
- On the Management >> General Settings page, click the "Security Option" tab.
- Verify the Password Complexity setting.

If the Password complexity setting is not set to Custom, with checkboxes enabled for uppercase letters, lowercase letters, numerical digits, and special characters, this is a finding.

Fix Text: Configure the Fly Server Manager security configuration:

- Log on to Fly Server with an admin account.
- On the Management >> General Settings page, click the "Security Option" tab.
- Set the Password Complexity setting to Custom, select four checkboxes to enforce that the password must contain four character types: uppercase letters, lowercase letters, digits, and special characters.

CCI: CCI-004066

Group ID (Vulid): V-283934

Group Title: SRG-APP-000170

Rule ID: SV-283934r1206156_rule

Severity: CAT II

Rule Version (STIG-ID): [FLYS-00-000090](#)

Rule Title: Fly Server must require the change of at least eight of the total number of characters when passwords are changed.

Vulnerability Discussion: If the application allows the user to consecutively reuse extensive portions of passwords, this increases the chances of password compromise by increasing the window of opportunity for attempts at guessing and brute-force attacks.

The number of changed characters refers to the number of changes required with respect to the total number of positions in the current password. In other words, characters may be the same within the two passwords; however, the positions of the like characters must be different.

Check Content:

Check the Fly Server Manager security configuration:

- Log on to Fly Server with an admin account.
- On the Management >> General Settings page, click the "Security Option" tab.
- Verify the Change Password setting is set to "New password cannot have consecutively same 8 characters as previous password".

If this option is unchecked, this is a finding.

Fix Text: Configure the Fly Server Manager security configuration:

- Log on to Fly Server with an admin account.
- On the Management >> General Settings page, click the "Security Option" tab.
- Set Change Password setting, check option "New password cannot have consecutively same 8 characters as previous password".

CCI: CCI-004066

Group ID (Vulid): V-283935

Group Title: SRG-APP-000173

Rule ID: SV-283935r1206159_rule

Severity: CAT II

Rule Version (STIG-ID): [FLYS-00-000095](#)

Rule Title: Fly Server must enforce 24 hours/1 day as the minimum password lifetime.

Vulnerability Discussion: Enforcing a minimum password lifetime helps prevent repeated password changes to defeat the password reuse or history enforcement requirement.

Restricting this setting limits the user's ability to change their password. Passwords must be changed at specific policy based intervals; however, if the application allows the user to immediately and continually change their password, then the password could be repeatedly changed in a short period of time to defeat the organization's policy regarding password reuse.

Check Content:

Check the Fly Server Manager security configuration:

- Log on to Fly Server with an admin account.
- On the Management >> General Settings page, click the "Security Option" tab.
- Verify the Change Password setting option "Change the password once only within 24 hours" is checked.

If this option is unchecked, this is a finding.

Fix Text: Configure the Fly Server Manager security configuration:

- Log on to Fly Server with an admin account.
- On the Management >> General Settings page, click the "Security Option" tab.
- Check "Change the password once only within 24 hours" to set the Change Password setting.

CCI: CCI-004066

Group ID (Vulid): V-283936

Group Title: SRG-APP-000190

Rule ID: SV-283936r1206162_rule

Severity: CAT II

Rule Version (STIG-ID): [FLYS-00-000100](#)

Rule Title: Fly Server must terminate sessions after 10 minutes.

Vulnerability Discussion: Terminating an idle session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console port that has been left unattended. In addition, quickly terminating an idle session will also free up resources committed by the managed network element.

Terminating network connections associated with communications sessions includes, for example, de-allocating associated TCP/IP address/port pairs at the operating system level, or de-allocating networking assignments at

the application level if multiple application sessions are using a single, operating system-level network connection. This does not mean that the application terminates all sessions or network access; it only ends the inactive session and releases the resources associated with that session.

Check Content:

Check the Fly Server Manager session setting:

- Log on to Fly Server Manager with an admin account.
- On the Management >> General Settings page, click the "System Option" tab.
- Verify the "Session Will Expire After Inactivity for:" setting is selected.

If this setting is not 10 minutes, this is a finding.

Fix Text: Configure the Fly Server Manager session setting:

- Log on to Fly Server Manager with an admin account.
- On the Management >> General Settings page, click the "System Option" tab.
- Set the session setting to "Session Will Expire After Inactivity for 10 minutes".

CCI: CCI-001133

Group ID (Vulid): V-283937

Group Title: SRG-APP-000291

Rule ID: SV-283937r1206895_rule

Severity: CAT II

Rule Version (STIG-ID): [FLYS-00-000105](#)

Rule Title: Fly Server must notify system administrators (SAs) and the information system security officer (ISSO) for all account-related events.

Vulnerability Discussion: Once an attacker establishes access to an application, the attacker often attempts to create a persistent method of reestablishing access. One way to accomplish this is for the attacker to simply create a new account. Sending notification of account creation events to the SA and ISSO is one method for mitigating this risk.

To address access requirements, many application developers choose to integrate their applications with enterprise-level authentication/access/auditing mechanisms that meet or exceed access control policy requirements. Such integration allows the application developer to off-load those access control functions and focus on core application features and functionality.

Satisfies: SRG-APP-000291, SRG-APP-000292, SRG-APP-000293, SRG-APP-000294, SRG-APP-000320

Check Content:

Check the Fly Server Manager Notification setting:

- Log on to Fly Server Manager with an admin account.
- On the Management >> Email Configuration, click the "Email Notification" tab.
- Verify "Send account management notification emails to:" is selected.

If this setting is not set, this is a finding.

Fix Text: Configure the Fly Server Manager Notification setting:

- Log on to Fly Server Manager with admin account.
- On the Management >> Email Configuration, click the "Email Notification" tab.
- Select the "Send account management notification emails to:" setting.
- Save the setting.

Group ID (Vulid): V-283938

Group Title: SRG-APP-000150

Rule ID: SV-283938r1223357_rule

Severity: CAT I

Rule Version (STIG-ID): [FLYS-00-000110](#)

Rule Title: Fly Server must have no local accounts for the user interface.

Vulnerability Discussion: To ensure accountability and prevent unauthenticated access, nonprivileged users must utilize multifactor authentication to prevent potential misuse and compromise of the system.

Multifactor authentication uses two or more factors to achieve authentication.

Factors include:

- (i) Something you know (e.g., password/PIN);
- (ii) Something you have (e.g., cryptographic identification device, token); or
- (iii) Something you are (e.g., biometric).

A nonprivileged account is any information system account with authorizations of a nonprivileged user.

Network access is any access to an application by a user (or process acting on behalf of a user) where said access is obtained through a network connection.

Applications integrating with the DoW Active Directory and utilize the DoW CAC are examples of compliant multifactor authentication solutions.

Satisfies: SRG-APP-000150, SRG-APP-000023, SRG-APP-000024, SRG-APP-000065, SRG-APP-000148, SRG-APP-000153, SRG-APP-000154, SRG-APP-000155, SRG-APP-000156, SRG-APP-000157, SRG-APP-000163, SRG-APP-000175, SRG-APP-000176, SRG-APP-000177, SRG-APP-000178, SRG-APP-000180, SRG-APP-000183, SRG-APP-000318, SRG-APP-000345, SRG-APP-000389, SRG-APP-000391, SRG-APP-000392, SRG-APP-000394, SRG-APP-000395, SRG-APP-000400, SRG-APP-000401, SRG-APP-000402, SRG-APP-000403, SRG-APP-000404, SRG-APP-000405, SRG-APP-000410, SRG-APP-000427, SRG-APP-000580, SRG-APP-000700, SRG-APP-000705, SRG-APP-000710, SRG-APP-000740, SRG-APP-000815, SRG-APP-000820, SRG-APP-000825, SRG-APP-000830, SRG-APP-000835, SRG-APP-000840, SRG-APP-000845, SRG-APP-000850, SRG-APP-000855, SRG-APP-000860, SRG-APP-000865, SRG-APP-000870, SRG-APP-000875, SRG-APP-000880, SRG-APP-000885, SRG-APP-000890

Check Content:

Once Active Directory is configured in FLYS-00-000055, all local users must be removed.

Check the Fly Server User settings:

- On the Management >> Account Manager tab, view the list of users.
- User accounts tied to an Active Directory domain will be defined as [domainname]\[username].

If any of the users listed are not tied to Active Directory, this is a finding.

Fix Text: Once Active Directory is configured in FLYS-00-000055, remove all local users:

- On the Management >> Account Manager tab, remove all local users.

CCI: CCI-000015

CCI: CCI-000016

CCI: CCI-000044

CCI: CCI-000764

CCI: CCI-004045

CCI: CCI-004046

CCI: CCI-001941

CCI: CCI-003627

CCI: CCI-000185

CCI: CCI-000186

CCI: CCI-000187

CCI: CCI-000206

CCI: CCI-000804

CCI: CCI-000884

CCI: CCI-002145

CCI: CCI-002238

CCI: CCI-002038

CCI: CCI-001953

CCI: CCI-001954

CCI: CCI-001958

CCI: CCI-001967

CCI: CCI-002007

CCI: CCI-004068

CCI: CCI-002009

CCI: CCI-002010

CCI: CCI-004083

CCI: CCI-004085

CCI: CCI-001632

CCI: CCI-002470

CCI: CCI-003628

CCI: CCI-003629

CCI: CCI-003747

CCI: CCI-004047

CCI: CCI-004058

CCI: CCI-004059

CCI: CCI-004060

CCI: CCI-004061

CCI: CCI-004062

CCI: CCI-004063

CCI: CCI-004064

CCI: CCI-004065

CCI: CCI-004066

CCI: CCI-004192

CCI: CCI-004901

CCI: CCI-004902

Group ID (Vulid): V-283939

Group Title: SRG-APP-000150

Rule ID: SV-283939r1223358_rule

Severity: CAT I

Rule Version (STIG-ID): [FLYS-00-000115](#)

Rule Title: Fly Server must have local authentication disabled.

Vulnerability Discussion: To ensure accountability and prevent unauthenticated access, nonprivileged users must utilize multifactor authentication to prevent potential misuse and compromise of the system.

Multifactor authentication uses two or more factors to achieve authentication.

Factors include:

- (i) Something you know (e.g., password/PIN);
- (ii) Something you have (e.g., cryptographic identification device, token); or
- (iii) Something you are (e.g., biometric).

A nonprivileged account is any information system account with authorizations of a nonprivileged user.

Network access is any access to an application by a user (or process acting on behalf of a user) where said access is obtained through a network connection.

Applications integrating with the DoW Active Directory and utilize the DoW CAC are examples of compliant multifactor authentication solutions.

Satisfies: SRG-APP-000150, SRG-APP-000023, SRG-APP-000024, SRG-APP-000065, SRG-APP-000148, SRG-APP-000153, SRG-APP-000154, SRG-APP-000155, SRG-APP-000156, SRG-APP-000157, SRG-APP-000163, SRG-APP-000175, SRG-APP-000176, SRG-APP-000177, SRG-APP-000178, SRG-APP-000180, SRG-APP-000183, SRG-APP-000318, SRG-APP-000345, SRG-APP-000389, SRG-APP-000391, SRG-APP-000392, SRG-APP-000394, SRG-APP-000395, SRG-APP-000400, SRG-APP-000401, SRG-APP-000402, SRG-APP-000403, SRG-APP-000404, SRG-APP-000405, SRG-APP-000410, SRG-APP-000427, SRG-APP-000580, SRG-APP-000700, SRG-APP-000705, SRG-APP-000710, SRG-APP-000740, SRG-APP-000815, SRG-APP-000820, SRG-APP-000825, SRG-APP-000830, SRG-APP-000835, SRG-APP-000840, SRG-APP-000845, SRG-APP-000850, SRG-APP-000855, SRG-APP-000860, SRG-APP-000865, SRG-APP-000870, SRG-APP-000875, SRG-APP-000880, SRG-APP-000885, SRG-APP-000890

Check Content:

Once Active Directory is configured in FLYS-00-000055, local authentication must be disabled.

- On the Management >> Account Manager tab, click "Authentication Manager".

If the slide-bar for Local System is active, this is a finding.

Fix Text: Once Active Directory is configured in FLYS-00-000055, disable local authentication:

- On the Management >> Account Manager tab, click "Authentication Manager".
- Disable the Local System slide-bar.

CCI: CCI-000766

CCI: CCI-000015

CCI: CCI-000016

CCI: CCI-000044

CCI: CCI-000764

CCI: CCI-004045

CCI: CCI-004046

CCI: CCI-001941

CCI: CCI-003627

CCI: CCI-000185

CCI: CCI-000186

CCI: CCI-000187

CCI: CCI-000206

CCI: CCI-000804

CCI: CCI-000884

CCI: CCI-002145

CCI: CCI-002238

CCI: CCI-002038

CCI: CCI-001953

CCI: CCI-001954

CCI: CCI-001958

CCI: CCI-001967

CCI: CCI-002007

CCI: CCI-004068

CCI: CCI-002009

CCI: CCI-002010

CCI: CCI-004083

CCI: CCI-004085

CCI: CCI-001632

CCI: CCI-002470

CCI: CCI-003628

CCI: CCI-003629

CCI: CCI-003747

CCI: CCI-004047

CCI: CCI-004058

CCI: CCI-004059

CCI: CCI-004060

CCI: CCI-004061

CCI: CCI-004062

CCI: CCI-004063

CCI: CCI-004064

CCI: CCI-004065

CCI: CCI-004066

CCI: CCI-004192

CCI: CCI-004901

CCI: CCI-004902

Group ID (Vulid): V-283941

Group Title: SRG-APP-000427

Rule ID: SV-283941r1223361_rule

Severity: CAT II

Rule Version (STIG-ID): [FLYS-00-000140](#)

Rule Title: Fly Server must only allow the use of DoW PKI established certificate authorities for verification of the establishment of protected sessions.

Vulnerability Discussion: Untrusted Certificate Authorities (CA) can issue certificates, but they may be issued by organizations or individuals that seek to compromise DoW systems or by organizations with insufficient security controls. If the CA used for verifying the certificate is not a DoW-approved CA, trust of this CA has not been established.

The DoW will only accept PKI certificates obtained from a DoW-approved internal or external certificate authority. Reliance on CAs for the establishment of secure sessions includes, for example, the use of TLS certificates.

This requirement focuses on communications protection for the application session rather than for the network packet.

This requirement applies to applications that use communications sessions. This includes, but is not limited to, web-based applications and service-oriented architectures (SOAs).

Satisfies: SRG-APP-000427, SRG-APP-000605

Check Content:

To validate the web certificate:

1. Run the following command to check sslcert:
curl.exe -vI https://<FLY host>:<port>/
2. If there is "The certificate chain was issued by an authority that is not trusted." in the output, this is a finding.

To validate the communication certificate:

1. Log in to the agent server.
2. Open the file "...\\APElements\\FLY\\Agent\\bin\\AgentCommonVCEnv.config" and find the value of

"agentSSLThumbprint".

3. Open the certmgr and find the certificate.

4. If the certificate is not a DoW PKI (or other AO-approved) certificate, this is a finding.

Fix Text: To replace the web certificate:

1. Prepare trusted certificate (pfx file).

2. Install the pfx certificate on the FLY Manager server.

3. Run the following command to replace the sslcert binding:

```
netsh http delete sslcert ipport=0.0.0.0:<FLY Manager Port default:20100>
```

```
netsh http add sslcert ipport=0.0.0.0:<FLY Manager Port default:20100> certhash=<THUMBPRINT> appid={b8a60d7f-c976-4416-b5af-f9e36cae4dae}
```

4. Update the value of the node "WebCertThumbprint" in the file ...

\FLY\Manager\Control\bin\TimerService.exe.config.

5. Restart "FLY Timer Service".

To replace the communication certificate:

1. Prepare trusted communication certificate (pfx file).

2. Install the pfx certificate on all FLY servers (agent and manager servers).

3. On the FLY Manager server, update the value of "CertThumbprint" in the file "...

\FLY\Manager\Control\bin\TimerService.exe.config".

4. Restart "FLY Timer Service".

5. Log in to the agent servers.

6. Run the following command to replace the sslcert binding:

```
netsh http delete sslcert ipport=0.0.0.0:<FLY Agent Port Default:20101>
```

```
netsh http add sslcert ipport=0.0.0.0:<FLY Agent Port Default:20101> certhash=<THUMBPRINT> appid={b8a60d7f-c976-4416-b5af-f9e36cae4dae}
```

7. Update the thumbprint in the following config file:

"agentSSLThumbprint" in ... \APElements\FLY\Agent\bin\AgentCommonVCEnv.config

"clientCertificate" and "serviceCertificate" in ...

\APElements\FLY\Agent\bin\AgentCommonWCFBehaviors.config

"clientCertificate" and "serviceCertificate" in ... \APElements\FLY\Agent\bin\CommonDataTransfer.config

8. Restart "FLY Agent Service".

CCI: CCI-002470

CCI: CCI-000185

Group ID (Vulid): V-283942

Group Title: SRG-APP-000516

Rule ID: SV-283942r1223359_rule

Severity: CAT III

Rule Version (STIG-ID): [FLYS-00-000150](#)

Rule Title: Fly Server must be configured to use an enterprise database solution.

Vulnerability Discussion: Configuring the application to implement organizationwide security implementation guides and security checklists ensures compliance with federal standards and establishes a common security baseline across DoW that reflects the most restrictive security posture consistent with operational requirements.

Configuration settings are the set of parameters that can be changed that affect the security posture and/or functionality of the system. Security-related parameters are those parameters impacting the security state of the application, including the parameters required to satisfy other security control requirements.

Check Content:

Check the Fly Server control database type in the configuration file of Fly Server manager:

Open "<Program Files>\APElements\FLY\Manager\Control\bin\TimerService.exe.config" with a text editor.

If the value of "ConfigDatabaseType" is "SQLite", the system has been configured to use built-in database when installing Fly Server manager.

If the value of "ConfigDatabaseType" is "SQLite", this is a finding.

If the value of "ConfigDatabaseInstance" points to a path local to the host where Fly Server resided, this is a finding.

Fix Text: Configure Fly Server to use a MS SQL server database when installing Fly Server manager. The MS-SQL server cannot reside on the same host as the Fly Server application.

CCI: CCI-000366

Group ID (Vulid): V-284007

Group Title: SRG-APP-000329

Rule ID: SV-284007r1207111_rule

Severity: CAT II

Rule Version (STIG-ID): [FLYS-00-000805](#)

Rule Title: Fly Server must enforce a role-based access control (RBAC) policy over defined subjects and objects.

Vulnerability Discussion: RBAC is an access control policy that restricts information system access to authorized users. Without these security policies, access control and enforcement mechanisms will not prevent unauthorized access.

Organizations can create specific roles based on job functions and the authorizations (i.e., privileges) to perform needed operations on organizational information systems associated with the organization-defined roles. When users are assigned to the organizational roles, they inherit the authorizations or privileges defined for those roles. RBAC simplifies privilege administration for organizations because privileges are not assigned directly to every user (which can be a significant number of individuals for mid- to large-size organizations) but are instead acquired through role assignments. RBAC can be implemented either as a mandatory or discretionary form of access control.

Pertains to Zero Trust.

Satisfies: SRG-APP-000329, SRG-APP-000233, SRG-APP-000328, SRG-APP-001040, SRG-APP-001045

Check Content:

RBAC hierarchy is to be defined by the authorizing official (AO). Separation of duties must be configured.

Check the Fly Server Role settings:

- Log on to Fly Server Manager with an admin account.
- On the Management >> Role Manager tab, view the configured roles.

If only one role exists, this is a finding.

Check the role assignments:

- On the Management >> Account Manager tab, view the Role column.

If only one role is assigned, this is a finding.

If only one user exists in the list of users, this is a finding.

Fix Text: RBAC hierarchy is to be defined by the AO. Separation of duties must be configured.

Configure the Fly Server Role settings:

- Log on to Fly Server Manager with an admin account.
- On the Management >> Role Manager tab, configure two or more roles.

Configure the role assignments:

- On the Management >> Account Manager tab, assign a unique role to two or more users. Add users if necessary.

CCI: CCI-002169

CCI: CCI-000366

CCI: CCI-001084

CCI: CCI-002165

CCI: CCI-003650

CCI: CCI-003652

Group ID (Vulid): V-284030

Group Title: SRG-APP-000456

Rule ID: SV-284030r1206442_rule

Severity: CAT II

Rule Version (STIG-ID): [FLYS-00-000950](#)

Rule Title: Fly Server must automatically check for updates weekly.

Vulnerability Discussion: Security flaws with software applications are discovered daily. Vendors are constantly updating and patching their products to address newly discovered security vulnerabilities. Organizations (including any contractor to the organization) are required to promptly install security-relevant software updates (e.g., patches, service packs, and hot fixes). Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling must also be addressed expeditiously.

Organization-defined time periods for updating security-relevant software may vary based on a variety of factors including, for example, the security category of the information system or the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw).

This requirement will apply to software patch management solutions used to install patches across the enclave and to applications themselves that are not part of that patch management solution. For example, many browsers today provide the capability to install their own patch software. Patch criticality, as well as system criticality will vary. Therefore, the tactical situations regarding the patch management process will also vary. This means that the time period used must be a configurable parameter. Time frames for application of security-relevant software updates may be dependent upon the Information Assurance Vulnerability Management (IAVM) process.

The application will be configured to check for and install security-relevant software updates within an identified time period from the availability of the update. The specific time period will be defined by an authoritative source (e.g., IAVM, CTOs, DTMs, and STIGs).

Check Content:

Check the Fly Server update service configuration:

- Log on to Fly Server with an admin account.
- On the Management >> System Information page, click "Service Configuration".
- Verify "Auto check new version" is set to "Weekly".

If the "Auto check new version" is not set to "Weekly", this is a finding.

Fix Text: Configure the Fly Server update service configuration:

- Log on to Fly Server with an admin account.
- On the Management >> System Information page, click "Service Configuration".
- Set "Auto check new version" to "Weekly".
- Click "Save".

CCI: CCI-002605

Group ID (Vulid): V-284031

Group Title: SRG-APP-000456

Rule ID: SV-284031r1206445_rule

Severity: CAT II

Rule Version (STIG-ID): [FLYS-00-000951](#)

Rule Title: Fly Server must be updated within 30 days of an update release.

Vulnerability Discussion: Security flaws with software applications are discovered daily. Vendors are constantly updating and patching their products to address newly discovered security vulnerabilities. Organizations (including any contractor to the organization) are required to promptly install security-relevant software updates (e.g., patches, service packs, and hot fixes). Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling must also be addressed expeditiously.

Organization-defined time periods for updating security-relevant software may vary based on a variety of factors including, for example, the security category of the information system or the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw).

This requirement will apply to software patch management solutions that are used to install patches across the enclave and also to applications themselves that are not part of that patch management solution. For example, many browsers today provide the capability to install their own patch software. Patch criticality, as well as system criticality will vary. Therefore, the tactical situations regarding the patch management process will also vary. This means that the time period used must be a configurable parameter. Time frames for application of security-relevant software updates may be dependent upon the Information Assurance Vulnerability Management (IAVM) process.

The application will be configured to check for and install security-relevant software updates within an identified time period from the availability of the update. The specific time period will be defined by an authoritative source (e.g., IAVM, CTOs, DTMs, and STIGs).

Check Content:

Check the Fly Server release version:

- Log on to Fly Server with an admin account.
- On the Management >> System Information page, click "Check for a new version".
- If a new version is available, the number will be displayed. Note the version number.
- Compare the new version number with the version history documented on AvePoint's website.

If no updated version information is displayed via "Check for a new version", the system is up to date. There is no finding.

If the available version number is more than 30 days old, this is a finding.

Fix Text: Upgrade the system:

- Log on to Fly Server with an admin account.
- On the Management >> System Information page, click "Check for a new version".
- If a new version is available, the number will be displayed. Note the version number.
- Compare the new version number with the version history documented on AvePoint's website.

Upgrade to the latest version within 30 days of release.

CCI: CCI-002605

Group ID (Vulid): V-284032

Group Title: SRG-APP-001035

Rule ID: SV-284032r1206448_rule

Severity: CAT I

Rule Version (STIG-ID): [FLYS-00-000952](#)

Rule Title: Fly Server must be a version supported by the vendor.

Vulnerability Discussion: Unsupported software and systems should not be used because fixes to newly identified bugs will not be implemented by the vendor. The lack of support can result in potential vulnerabilities.

Software and systems at unsupported servicing levels or releases will not receive security updates for new vulnerabilities, which leaves them subject to exploitation.

When maintenance updates and patches are no longer available, software is no longer considered supported and should be upgraded or decommissioned.

Check Content:

Check the Fly Server release version:

- Log on to Fly Server with an admin account.
- On the Management >> System Information page, note the version number.
- Compare the version number with the product end of life information documented on AvePoint's website.

If the version information is displayed is not supported by the vendor, this is a finding.

Fix Text: Upgrade the system to a supported version.

CCI: CCI-003376

UNCLASSIFIED