egress

switch
secure data exchange

Egress Switch

Best Practice Security Guide

Confidentiality Statement

This document contains information confidential and proprietary to Egress Software Technologies. It shall not be disclosed in whole or part by the recipient to any third party or to any employees other than those who have a need to know such information. It shall not be duplicated or used by the recipient for any purpose other than to evaluate Egress Software Technologies products and services.

No part of this document may be reproduced, distributed, stored in a database or retrieval system, or transmitted in any form or by any means, without the exclusive and written permission of Egress Software Technologies. No liability is assumed for damages resulting from the use of the information contained herein.

Copyright Notice

Contents

Introduction

This document is a guide to implementing and maintaining an Egress Switch secure data exchange infrastructure, covering best practice security, recommendatory and mandatory policies.

Best practice installation

The following section covers best practice deployment recommendations for the Egress Server Infrastructure (ESI), Switch Gateway and Switch Client software. The following guidelines will ensure high levels of security and resilience are maintained.

Software updates

Egress Software issues regular software updates to all applications. It is highly recommended you ensure that the latest updates are applied routinely where possible. Additionally, any critical security hot fixes should be applied as a matter of urgency. It is recommended that system administrators subscribe to the Egress' product updates and service notifications service from within their Switch ID account settings.

Please also ensure that all updates are only ever received via an authorised Egress source including http://support.egress.com. Thorough testing should be performed before applying any updates and these will never be applied automatically.

Operating system service packs & hot fixes

All workstations and servers must be running the latest Service Packs and hot fixes from Microsoft. Egress Software Technologies regularly issue security bulletins and updates to the core installers to ensure that any security relevant updates are applied.

Signature verification

For Microsoft Windows Operating Systems, it is highly recommended that signature verification is enabled for applications, services and drivers in the host OS. For further information please visit the Microsoft at www.microsoft.com.

Enable Address Space Layout Randomisation (ASLR)

ASLR is enabled by default in Windows OS since Windows Vista (2009). It is recommended that ASLR is enabled for enhanced system security. All Egress Switch components are ASLR friendly and will use the technology if supported by the OS.

Anti-virus/anti-malware software

Ensure that all workstations and servers have up to date anti-virus software with the latest malware definitions and libraries.

Authentication safeguards

Appropriate Operating System security must exist on all desktops and servers before Egress Switch is deployed. This includes, but is not limited to correct implementation of OS access controls, network privileges and physical security.

Certificates

Dependant on configuration, certificates maybe required as part of the core ESI installation. Certificates should only be obtained from authorised certificate authorities.

System administrators

System administrators of the ESI should receive appropriate training from Egress Software Technologies or an authorised partner. Training will cover the following tasks:

- Day to day management of the ESI and Switch Gateway
- User management including enrolment, deletion and permission changes
- Policy management
- Fault finding and log analysis
- Deployment and management of Switch client software

All system administrator actions including policy modifications and user actions are audited and tamper proof.

Audit analysis

The ESI, Switch Gateway and Switch Client apps maintain detailed audit logs of security related events, system internal events and performance information.

System administrators should perform regular reviews of the audit lots for unexpected events and action investigations accordingly. This should also cover suspected tampering and security related incidents.

Key management

Egress Switch users an advanced Key Management System utilising AES 256 bit data encryption and SSL authentication. Whilst most key management procedures are performed automatically by the core software, there may be requirements for authorised system administrators to perform certain tasks.

Egress Switch does not issue asymmetric keys to users but instead users AES encryption and integrity validation, with pseudo-random keys issued for individual packages. The key for existing packages can be revoked by sender and/or system administrator using the management interface.

User management is performed by authorised system administrators using the Switch Management interface. Procedures should be implemented to control user enrolment, user expiration, deletion and revocation of secure information.

Database encryption keys, password or secrets utilised by service components are all stored by the Switch Server and Gateway in keychain.xml file. Using the keychain utility provided, system administrator may add new encryption keys when the existing keys are at the end of their service life or in the event of potential compromise.

End users

The Egress Switch client software has been designed to integrate with existing systems and applications without the requirements for elevated system privileges. Egress Switch will be seamlessly integrated with existing business process and applications.

It is recommended that end users receive a basic level of training on how to send secure email and files covering best practice and how to recognise potential security vulnerabilities. Egress Software Technologies provide a number of user guides/training, FAQs and useful video tutorials. These can be found at http://www.egress.com/support/.

Furthermore, organisations should embrace their own tailored training and awareness campaigns prior to deployment of Egress' products. This will minimise the risk of security exploitations and keep and phishing attacks and system malfunction to an absolute minimum. In addition, users must have the minimum level of privileges to perform their daily tasks.

Clear procedural documentation should be provided to all users detailing the following:

- How to recognise potential security problems/breaches.
- How to use the software.
- Clear direction should be advised on how to report security incidents. These should also be audited.

Password security

Passwords are required in various components of both the Egress Switch core infrastructure setup (service accounts etc.) and in general use by users of the system to secure Switch IDs.

It is highly recommended that strong passwords are to be used. These should be mandated in the ESI policy, according to the following guidelines:

Keys to password strength: length & complexity

An ideal password is lengthy and incorporates a mixture of numbers, letters, punctuation and symbols:

- Aim to incorporate a minimum of eight characters of more.
- Do not use the same password across multiple accounts. Cybercriminals can hack into passwords with very little security with ease.
- Change your passwords often i.e. every 60 days. Set an automatic reminder to change your passwords, particularly on banking, email and credit card company websites.
- The greater the variety of characters in your password, the more secure it will be. However, password hacking software automatically checks for common letter-to-symbol conversions, such as changing “and” to “&” and “to” to “2”.
- Attempt to use the entire keyboard, not just letters and characters you use or see most often.

Common password pitfalls to avoid

Cybercriminals use sophisticated tools that can rapidly decipher passwords. Avoid at all times using passwords that use the following:

- Dictionary words in any language
- Words spelled backwards, common misspellings and abbreviations
- Sequences or repeated characters. Examples: 12345678, 2222222, abcdefg or adjacent letters on your keyboard such as QWERTY.
- Personal information: name, birthday, passport number or similar information which could easily be predicted.

Uninstallation (disposal & destruction)

In the event that you need to uninstall Egress Switch software, careful consideration should be given to decommissioning the various components.

Egress Switch Server Infrastructure: The Egress Switch Server Infrastructure is the core component for a Switch Installation. The server infrastructure holds key encryption data, policies and user credentials. While all data is stored in encrypted format consideration should be given to appropriate end of life decommissioning.

The uninstallation can be performed from Add/Remove Programs/Program Features that will securely remove the complete infrastructure.

Important Note: The Uninstallation of Egress Server Infrastructure cannot be reversed so please proceed with caution and ensure appropriate data backups have been performed and checked.

Egress Switch Gateway: The Egress Switch Gateway can be uninstalled using Add/Remove Programs/Program Features. As Switch Gateway does not hold persistent encryption keys this can be uninstalled securely and reinstalled if necessary.

Egress Switch Client: The Egress Switch client can be uninstalled cleanly and securely using Add/Remove Programs/Program Features.

Switch support centre

Should you encounter any problems with Egress Switch please visit the Egress Software Technologies Support Centre www.egress.com/support.

Useful contact information:

Egress Europe:	+44-844-8000-172
Egress North America:	1-888-505-8318
Egress Australia:	1-800-768-043
Egress Singapore:	800-130-2208
Egress Website Address:	http://www.egress.com
Egress Sales:	sales@egress.com
Account Services:	accountservices@egress.com
Support:	support@egress.com
Follow Egress Online:	Twitter Facebook LinkedIn Egress Blog