***Contact Center Operations***

eCL AdminWeb Application

Implementation Run Book

|  |  |
| --- | --- |
| Description | **TFS 5919 – Move the current functionality of the current Access Control List to the Admin Tool** |

##### Contents

[Overview 1](#_Toc452963680)

[Implementation Steps 1](#_Toc452963681)

[Important Notes 2](#_Toc452963682)

[Appendix: 3](#_Toc452963683)

##### Revision History

|  |  |  |
| --- | --- | --- |
| Date | Change Description | Author |
| 06/06/2016 | TFS 2527 - eCL Admin Tool.  (Inactivate/Reactivate/Reassign logs) | Lili Huang |
| 12/02/2016 | TFS 3841 (Parent 3027) – Added Sr. Mgr. Dashboard | Lili Huang |
| 4/24/2017 | TFS 5421 - Delete logs;  TFS 5420 - Reporting;  TFS 5621 - Initial Reporting. | Lili Huang |
| 05/01/2017 | TFS 5919 – Move the functionality of the current Access Control List to the Admin Tool | Lili Huang |

|  |
| --- |
| Overview |

|  |  |
| --- | --- |
| Purpose: | The purpose of this run book is to provide a documented process and instruction on how authorized CCO Engineers should implement GDIT-developed changes for eCL Admin Web Application per TFS TFS 5919 – Move the functionality of the current Access Control List to the Admin Tool. |
| Change Summary: |  |
| Dependencies: | None |
| Affected Server(s): | PROD Web Server: f3420-mwbp11.vangent.local  PROD DB Server: VDENSSDBP07\SCORP01,1436 |
| Security Impact: | None |
| Access Level Needed: | Implementer needs:   * TFS access |

|  |
| --- |
| Implementation Steps |

|  |  |
| --- | --- |
| Purpose/Scope: | This process describes the steps taken to implement changes to eCL Admin Web Application in the production environment for TFS 5919. |
| Responsibility: |  |
| References / forms/ documents: | In TFS:   * <eCoaching\_V2\Code\DB\Stored Procedures\sp\_HistoricalDashboardAclInsert.sql> – **Changeset 37258** * **<**eCoaching\_V2\UI Code\eCLAdmin\_publish.zip> - **Changeset 37263** |
| Preconditions: | None |
| Procedure: |  |
| Step 1: | Using SQL Server Management Studio or another query tool, connect to the appropriate environment database and run the following SQL scripts from TFS, noting the current version of the file to use from the referenced documents above. Run them in the order listed here.  sp\_HistoricalDashboardAclInsert.sql |
| Step 2: | **For Production implementation only:**  RDC to Production server: f3420-mwbp11.vangent.local;  Go to the IIS application server and filter access to prevent any user access except for the tester’s IP address;  *See Appendix on “How to add IP restrictions to deny access to eCL Admin site”* |
| Step 3: | **For Production implementation only:**  Backup folder D:\inetpub\wwwroot\eCLAdmin;  Delete all files under D:\inetpub\wwwroot\ eCLAdmin except:   * web.config   Unzip eCLAdmin\_publish.zip to folder D:\inetpub\wwwroot\ eCLAdmin, **do not overwrite web.config**. |
|  |  |
| Step 4: | **For Production implementation only:**  Notify tester to test. |
| Step 5: | **For Production implementation only:**  Once tester has given approval, go to the IIS application server and update filter to allow all user access.  *See Appendix on “How to remove IP restrictions”* |
| Step 6: | Notify program. |
|  |  |
|  |  |
| Post-conditions: | None |
|  |  |

|  |
| --- |
| Important Notes |

|  |  |
| --- | --- |
| Purpose/Scope: | This section lists any other items of note for the implementation. |
| Note 1: |  |
| Note 2: |  |
|  |  |

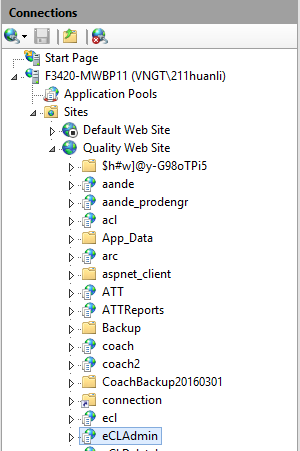
# Appendix:

**How to add IP restrictions to deny access to eCL Admin site**

1. Remote Desktop Connect to production web server.
2. Open **Internet Information Services (IIS) Manager**:

* On the taskbar, click **Server Manager**, click **Tools**, and then click **Internet Information Services (IIS) Manager**.

1. In the **Connections** pane, expand the server name, expand **Sites**, and then **Quality Web Site**, **eCLAdmin**.

****

1. In the **Home** pane, double-click the **IP Address and Domain Restrictions** feature.



1. In the **IP Address and Domain Restrictions** feature, click **Edit Feature Settings…** in the **Actions** pane. Select **Deny** for **Access for unspecified clients:** dropdown, click OK.



1. Click **Add Allow Entry…** in the **Actions** pane, enter the **IP** address that you wish to allow, and then click OK.

****



**How to remove IP restrictions**

1. In the **IP Address and Domain Restrictions** feature, click **Edit Feature Settings…** in the **Actions** pane. Select **Allow** for **Access for unspecified clients:** dropdown, click OK.



1. In the **IP Address and Domain Restrictions feature**, select the IP address added in step 6, and click **Remove** in the Actions pane.

****