

James Miller

James.miller[@callcreditgroup.co](mailto:Adrian.hall@callcreditgroup.com)m

Document Classification: Strictly Confidential

**Project Newcastle High Level Design**

*A high-level view of the IT solution supporting the project Newcastle Divestment*

[0 Document Control 3](#_Toc531355961)

[0.1 Revision History 3](#_Toc531355962)

[0.2 Approval and Sign-Off 3](#_Toc531355963)

[0.3 Reviewers/Distribution 3](#_Toc531355964)

[0.4 References 4](#_Toc531355965)

[0.5 Abbreviations 4](#_Toc531355966)

[1 Introduction 5](#_Toc531355967)

[1.1 Summary 5](#_Toc531355968)

[1.2 Document Purpose 5](#_Toc531355969)

[1.3 Target Audience 5](#_Toc531355970)

[1.4 In-Scope 5](#_Toc531355971)

[1.5 Out of Scope 5](#_Toc531355972)

[1.6 Key Technical Requirements 5](#_Toc531355973)

[1.7 Technical R.A.I.D Log 6](#_Toc531355974)

[1.7.1 Risks 6](#_Toc531355975)

[1.7.2 Issues 6](#_Toc531355976)

[1.7.3 Assumptions 6](#_Toc531355977)

[1.7.4 Dependencies 7](#_Toc531355978)

[1.8 Requirements Mapping 7](#_Toc531355979)

[2 Solution Overview 8](#_Toc531355980)

[2.1 Introduction 8](#_Toc531355981)

[2.2 Current State 8](#_Toc531355982)

[2.3 Transition State 8](#_Toc531355983)

[2.4 End State 8](#_Toc531355984)

[3 Design Summary 9](#_Toc531355985)

[3.1 Design PrincIples 9](#_Toc531355986)

[3.2 Design Decisions 9](#_Toc531355987)

[3.3 Security Controls 9](#_Toc531355988)

[4 Client Remote access 10](#_Toc531355989)

[4.1 Client Internet Connectivity 10](#_Toc531355990)

[4.2 VPN Gateway Internet Connectivity 10](#_Toc531355991)

[4.3 Cisco AnyConnect 10](#_Toc531355992)

[4.4 Security Controls 11](#_Toc531355993)

[5 End user compute 13](#_Toc531355994)

[5.1 Microsoft Windows 8 13](#_Toc531355995)

[5.2 Security Controls 13](#_Toc531355996)

[6 microsoft office 365 & collaboration 14](#_Toc531355997)

[6.1 Domains and configuration 15](#_Toc531355998)

[6.2 Email Hygiene and Routing 15](#_Toc531355999)

[6.3 Skype for Business 15](#_Toc531356000)

[6.4 Intune 15](#_Toc531356001)

[6.5 Multi factor authentication 16](#_Toc531356002)

[7 Microsoft Active Directory 17](#_Toc531356003)

[7.1 Group Membership 17](#_Toc531356004)

[7.2 Group Policy 19](#_Toc531356005)

[8 USER EXPerience 20](#_Toc531356006)

[8.1 User Accounts 20](#_Toc531356007)

[8.2 User Devices & Desktop Build 20](#_Toc531356008)

[8.3 Internet Access 20](#_Toc531356009)

[8.4 User Applications 21](#_Toc531356010)

[8.5 Cisco Anyconnect 21](#_Toc531356011)

[8.6 Email 21](#_Toc531356012)

[8.7 Sharepoint 22](#_Toc531356013)

[8.8 ONEDRIVE for business 22](#_Toc531356014)

[8.9 Cryoserver 22](#_Toc531356015)

[9 data Migration 23](#_Toc531356016)

[9.1 Policy 23](#_Toc531356017)

[9.2 Process 23](#_Toc531356018)

[9.3 Dual Running 23](#_Toc531356019)

[10 Software LICENSING 24](#_Toc531356020)

[11 Design Decisions & Issues Backlog 25](#_Toc531356021)

[11.1 Design Decisions 25](#_Toc531356022)

[11.2 Issues Backlog 25](#_Toc531356023)

[11.3 Outstanding Questions Log 25](#_Toc531356024)

[11.4 Post-Design Points/Activities 25](#_Toc531356025)

[Appendix A Project Delivery sequence 26](#_Toc531356026)

# Document Control

## Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Issue Date** | **Type of Change** | **Author** |
| 0.1 | 30/11/2017 | Initial Draft / Baseline solution overview | James Miller |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Approval and Sign-Off

Signatures on this document imply that you have read and understand the contents.

Approvers must review and sign off. Sign-off formally confirms the content is stated correctly.

This document must be approved by:

|  |  |  |  |
| --- | --- | --- | --- |
| **Role** | **Name(s)** | **Approval Date** | **Version Approved** |
| IT Technology Change Programme Team | Sinclair Elliot |  |  |
| Service Improvement Manager | Chris Wilson |  |  |
| Principal – IT Security | Kieran Brady |  |  |
| Head of Service Strategy | Ben Waterfall |  |  |
| Head of IT Operations | Mike Prescott |  |  |
| Head of Distributed IT Services | Jay Patel |  |  |
| Head of IT Service Management | Matt Tordoff |  |  |
| Newcastle TSA Manager, IT Operations | Mark Slocombe |  |  |

## Reviewers/Distribution

Names listed below included for review and feedback as required:

|  |  |
| --- | --- |
| **Name** | **Role** |
| Adrian Hall | Infrastructure Architect |
| Andrew Wilson | Andrew Wilson |
| David Hotchkiss | System & Platform Build |
| David Money | System Build Engineer (Noddle) |
| David Silkstone | Service Delivery Management |
| David Wilson | Product Architecture |
| Gary Naylor | Service Design Architect |
| Ian Mason | Senior Engineer - Infrastructure |
| Ian Stephenson | Head of Product Delivery (Noddle) |
| James Connors | Test Engineer |
| James Wood | Senior Information Security Analyst |
| Jay Patel | Head of Distributed IT Services |
| Kieran Brady | Manager - Security Management & Standards |
| Mike Prescot | Head of IT Operations |
| Neil Fitzgerald | Product Development Manager (Noddle) |
| Nic Mesa | IT Director |
| Paul Hoyland | Senior Network Engineer |
| Scott Clarke | Senior Infrastructure Engineer |
| Steven Powell | Network Architect |
| Suky Matharu | Suky Matharu |

## References

All references supporting this document are in the [Newcastle Project SharePoint](https://callcreditgroup.sharepoint.com/coo/etd/Project%20%20Newcastle/Forms/AllItems.aspx).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Document Name** | **Purpose** | **Publishing Org/Author** | **Filename** |
| R1. | Transitional Services Agreement | Definition of Contractual services to be supplied by TU UK. | TU UK | TSA - 26 10 18 (FN52598).pdf |
| R2. | Current Noddle User List & Inventory | Per User List of hardware assets (laptop/desktop/PC & Mobile) | Suky Matharu | Project Newcastle User List.xls |
| R3. | Security Requirements | Newcastle Security Requirements | Kieran Brady | Newcastle-Security Requirements-V0.1.doc |
| R4. | Transitional Services Requirements Mapping | TSA Requirements | Andrew Wilson | Newcastle Requirements Mapping.xls |
| R5. | Application Access Requirements | Inventory of Applications required during the TSA period | Andrew Wilson | Access requirements.xls |
| R6. | Collaboration Tooling Proposal | Proposal for provision of new Office 365 Tenant services. | Scott Clarke | Newcastle\_O365\_Concept\_Prose.doc |
| R7. | Remote Access Solution Overview | Noddle Remote Access Connectivity | Steven Powell/Paul Hoyland | Newcastle Network Proposal 0.1.ppt |

## Abbreviations

|  |  |
| --- | --- |
| **Acronym** | **Definition** |
| 1FA | Single Factor Authentication |
| 2FA | Two Factor Authentication |
| AD | Active Directory |
| CIG | Callcredit Information Group |
| CRL | City Road London |
| O365 | Microsoft Office 365 |
| PLL | Park Lane Leeds |
| SLA | Service Level Agreement |
| TSA | Transition services Agreement |
| TU UK | TransUnion UK |
| VAL | Volt Avenue London |
| VPN | Virtual Private Network |

# Introduction

## Summary

The primary objective of Project Newcastle is to support the divestment of the Noddle Business to the new owner Newcastle and provide for the IT services defined in the Transitional Services Agreement between Transunion and Call Credit Consumer Limited for the specified duration.

The Divestment will be delivered in a sequence of phases with the initial focus upon the seamless transition of Noddle employees from TransUnion UK Park Lane office to a new location in Leeds whilst providing for continued access to Transunion IT systems and services.

The IT services that specified in the Transitional Services Agreement have been identified as follows:

* Systems Access, Access Control and Network Segregation
* Collaboration
* Data
* Hardware, Software and Licensing
* Information Security
* Product Platform Management and Separation
* User Support/Product Support/Professional Services
* Reporting

## Document Purpose

To provide a high-level overview of the continued provision of Transunion UK (TU UK) IT services as specified in the Transitional Services Agreement (TSA) covering the underlying technical solution comprising of Remote Access Connectivity, End User Compute, Microsoft Office 365 & Collaboration and Active Directory.

## Target Audience

This document is aimed at providing a solution overview of the end to end IT solution and sufficient level of detail for Network and Infrastructure teams at TU UK to be able to produce low-level designs as required to enable the implementation of all solution components.

## In-Scope

* Provision of IT related services for the TSA term as per ‘requirements’ in the TSA schedules
* Provision of IT support for the separation of Noddle from the core business by the end of the TSA
* Provision of a re-commissioned laptop build to Noddle employees
* Provision of continued access to TU UK IT systems

## Out of Scope

* Credit View (Subject to a later transition phase)

## Key Technical Requirements

The following list summarises the key technical requirements that are satisfied as part of this design.

* Remote Access connectivity solution to provide for continued access to TU UK network and resources.
* Provision of a new CIG desktop device to provide for continued access to TU UK network and resources.
* Active Directory design to provide for the separation of Noddle users, security policies and user permissions
* Provision of a new Microsoft Office 365 Tenant with sufficient licenses to operate all required services secured with Azure conditional access.

## Technical R.A.I.D Log

### Risks

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Ref** | **Description** | **Likelihood [L/M/H]** | **Impact**  **[L/M/H]** | **Mitigation** |
|  | **Global** |  |  |  |
|  | The major risk posed by redeploying the Divesting business onto a new Network and Active Directory profile is business continuity should loss of systems access result. | H | H | Mitigation of functional access to existing systems will be subject to sufficient time to conduct a PoC incorporating Audit and User Acceptance Testing prior to go-live. |
|  | **Remote Access** |  |  |  |
|  | Large File Transfers through the VPN Tunnel could impact the availability of the service | M | M | User training and awareness |
|  | TU UK build updates / patching on VPN could impact availability | M | M | Schedule updates outside of core business hours |
|  | Unplanned Events / Disaster Recovery may oversubscribe the Remote access solution. | L | H | This business risk will be mitigated with the re-provision of the remote access solution to the new Corporate Hubs which will partition Internet bandwidth between Corporate and Product needs. |
|  | The PLL Internet bandwidth may be saturated by the Noddle Remote access VPN profile | L | H | This scenario will be mitigated with the forthcoming bandwidth upgrade of PLL internet provision with Vodafone (300=>500Mbps) |
|  | The PLL Internet bandwidth upgrade outside timeframe of go-live | M | L | It is envisaged that traffic profile will be sustainable for the concurrency expected < 40 users concurrent approx. |
|  | The Hairpin of VPN traffic from AnyConnect to Microsoft Azure/Ensono through PLL firewall FWL5. | L | L | The routing of traffic in/out of PLL firewall FWL5 will be subject to PoC and may require alternate traffic engineering should issues be encountered. |
|  | Measurement of network parameters not sufficient to validate against Service Level Agreements. | M | L | TU UK will need to demonstrate the health of the VPN service boundary which may require additional tools and monitoring capabilities. |

### Issues

|  |  |  |  |
| --- | --- | --- | --- |
| **Ref** | **Description** | **Mitigation / Status** | **Owner** |
|  | **Remote Access** |  |  |
|  | TU UK Skype currently has no site resiliency (PLL based) | The lack of TU UK resilience for the on-premise Skype platform should not impact Noddle users migrating to Microsoft O365 shared service. | IT Business Systems |
|  | Proxy currently has no site resiliency (PLL based) | This issue will be mitigated by the Integration project and corporate hubs to be located in VAL/CRL. | IT Business Systems |

### Assumptions

|  |  |  |
| --- | --- | --- |
| **Ref** | **Description** | **Verified** |
|  | **Remote Access** |  |
|  | All Facilities Management related to the new Noddle Office premises including Internet access, bandwidth capacity and availability will be the responsibility of Newcastle. | New Owner Newcastle will be responsible for the provision of the new Office Facilities and Internet Access. |
|  | The Technical Services Agreement IT service provision will be based upon a 12-month period (Oct 2017-Oct 2018). | TSA Contractual Requirement |

### Dependencies

|  |  |  |
| --- | --- | --- |
| **Ref** | **Description** | **Owner(s)** |
|  | **Remote Access** |  |
|  | Newcastle new Office facilities provide for a suitable Internet solution i.e. bandwidth and availability to support 45-60 employees. | Newcastle |
|  | TU UK VPN headend capacity in both Park Lane Leeds and Elland is sufficient to support combined corporate and remote access requirements for the duration of the TSA. | TU UK Operations |

## Requirements Mapping

This document reflects the provision of the initial delivery of the TU UK IT services to Newcastle required to continue operations following Financial Conduct Authority approval of the divestment.

The following requirements as specified in the Transitional Services Agreement schedule 7 are met as follows.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| No | Schedule | Sub Schedule | Compliant  Yes/No | Design Reference |
| 7 | EUIT End User IT Support | EUIT001 New user setup and provisioning (Joiners, Movers and Leavers process) |  |  |
| 7 | EUIT End User IT Support | EUIT002 Provision and support of End User Computing equipment | Yes | Section 5 |
| 7 | EUIT End User IT Support | EUIT003 Software License Management |  |  |
| 7 | EUIT End User IT Support | EUIT004 E-mail Services | Yes | Section 6 |
| 7 | EUIT End User IT Support | EUIT005 Migration of E-mail | Yes | Section 9 |
| 7 | EUIT End User IT Support | EUIT006 End User IT Service Desk |  |  |
| 7 | EUIT End User IT Support | EUIT007 End User Security Training |  |  |
| 7 | EUIT End User IT Support | EUIT008 Mobile Phone Service | Yes | Section 6.4 |
| 7 | EUIT End User IT Support | EUIT009 WIFI/ VPN other remote access | Yes | Section 4 |
| 7 | EUIT End User IT Support | EUIT010 Data Purging Project |  |  |
| 7 | EUIT End User IT Support | EUIT011 File Storage Provision | Yes | Section 8.7, 8.8 |
| 7 | EUIT End User IT Support | EUIT012 Account Management |  |  |
| 7 | EUIT End User IT Support | EUIT013 Telephony Services | Yes | Section 6.3 |
| 7 | EUIT End User IT Support | EUIT014 Unified Communication |  |  |
| 7 | EUIT End User IT Support | EUIT015 Printers |  |  |
| 7 | EUIT End User IT Support | EUIT016 Security & Identity & Access Management | Yes | Section 7 |
| 7 | EUIT End User IT Support | EUIT017 Professional Services |  |  |

# Solution Overview

## Introduction

The solution will provide for continued access to TU UK systems detailed in the TSA service schedules underpinned by the technical workstreams (Remote Access, Office & Collaboration, End User Compute and Active Directory) illustrated in the figure below.



Figure 1.0 - Current State Architecture

## Current State

The existing Noddle employees are subject to standard TU UK IT services including both wired, wireless and remote access methods providing for full access to TU UK internal and external systems.

## Transition State

During the TSA period the Noddle employees will be provided with a new divestment posture securely separating the business comprising of a new TU UK provided corporate machine, remote access VPN and new Active Directory accounts/groups based upon a least privileges security principle whilst also removing all TU UK data prior to the divestment commencement.

## End State

Before the end of the TSA period the Noddle employees will transition all TSA services to Newcastle returning all TU UK assets.

# Design Summary

To provide single view of the design elements covered within this document, the following sections present the Design Principles, Decisions and Security Controls followed by a detailed breakdown of each solution component.

## Design PrincIples

* All hardware and software to support the delivery of the TSA services will be provided where possible by existing TransUnion standard procurement and licensing agreements.
* All Office Facilities Management, Internet access, bandwidth capacity and availability will be the responsibility of Newcastle.

## Design Decisions

The key decisions supporting this high-level design are presented full in Section 11.1 and summarised as follows.

* All divesting users will be provided with a new TU UK Windows 7 desktop build
* The connectivity solution will be TU UK standard remote access (Cisco AnyConnect Full Tunnel VPN)
* The connectivity solution will whitelist access to approved TU UK resources
* All divesting users will receive a new Active Directory account
* All divesting users will receive new Active Directory Groups controlling access to TU UK resources
* All divesting users with both Laptop and PCs will received a single developer specification Laptop

## Security Controls

The solution design provides for a number of security controls which segment the Noddle business from the TU UK network providing for a secure Divestment posture whilst operating within the TSA period.

The security controls detailed within this design document are summarised as follows.

* Provision of a new TU UK CIG device secured with a Divestment posture as follows.
  + No access to Team Shares (V, W,X Y X)
  + Internet access secured via TU UK Forcepoint Proxies (McAfee)
  + Active Directory Group Policies blocking access to PLL WIFI networks
* Provision of a new Remote access solution secured with a Divestment posture as follows.
  + Device authentication using existing TU UK issued machine certificate
  + Two factor user authentication (CIG user and RSA Token)
  + New IP Subnet assigned to all Noddle employees
  + Per Device/User firewall policy permitting access to whitelisted TU UK resources
* Provision of new Active Directory accounts for each divesting employee
* Provision of new Active Directory groups granting access to approved TU UK resources
* Provision of a new O365 Tenant providing for Mail, Office and Collaboration services
* Access to new O365 Tenant restricted to TU UK network (O365 Conditional Access)
* Access to new O365 Tenant restricted to TU UK devices (installed with a valid machine certificate)

# Client Remote access

The remote access solution will provide for the continued access to access all TU UK resources as defined in the TSA providing for the following.

* Provision of a Cisco AnyConnect Client to Site VPN with full tunnel (no split tunnel permitted)
* Connectivity support for 45 employees increasing to 60 over the TSA term
* New Remote Access Profile and Subnet providing for Separation of access to approved TU UK resources
* Device authentication via existing TU UK internal CA issued Machine Certificate
* User authentication via TU UK Active Directory and RSA soft token (2FA)

## Client Internet Connectivity

The Internet access provision will provide for connectivity to the TU UK VPN either whilst roaming, working from home or whilst from the new Newcastle offices in Leeds.

Access from the Newcastle office premises will depend upon the local internet access provision and therefore it is imperative that the local internet connection provides for both sufficient bandwidth and availability to support up to 60 employees concurrently connected to the Cisco AnyConnect VPN.

## VPN Gateway Internet Connectivity

The existing TU VPN headend will be leveraged to support the Noddle Divestment located in both Park Lane Leeds (Primary Site) and Elland (Disaster Recovery Site) with a Park Lane Internet bandwidth provision of 300Mbps which in turn is pending an upgrade from the Service Provider (Vodafone) to 500Mbps.

In the medium term the Park Lane Internet bandwidth provision is shared with Corporate and Product internet access requirements and therefore the solution assumes for sufficient bandwidth availability to support Remote Access, Corporate and Product Internet access demand.

In the longer term the Remote Access solution shall be re-located to the TU UK network hubs to be located in both London Data Centres (CRL & VAL) which will comprise of dedicated corporate Internet bandwidth mitigating the current contention scenario present in Park Lane.

## Cisco AnyConnect

The VPN solution is based upon the Cisco AnyConnect client which will be deployed with a Dynamic Access Policy providing for a Noddle specific profile that will require the following.

1. Valid Machine Certificate (Device)
2. Valid CIG Active Directory (User 1FA)
3. Valid CIG RSA Soft Token (User 2FA)

The new Cisco AnyConnect profile will be configured to permit access based upon the following.

1. User Device Has TU UK Certificate installed
2. User is a member of the required Active Directory Security Group (CIG.VPN.Noddle) / Organisational Unit and possess a valid RSA token

Once the above criteria are satisfied the Client device will then be connected to the VPN and assigned an address from the Noddle IP subnet.

## Security Controls

The DHCP Scopes to be reserved for the Noddle VPN profile are presented in the tables below.

|  |  |
| --- | --- |
| **Variable** | **Assignment** |
| Start Address | 172.31.6.10 |
| End Address | 172.31.6.120 |
| Subnet Mask | 255.255.255.128 Length: 25 |

Table 0.1 – Park Lane Leeds DHCP Scope

|  |  |
| --- | --- |
| **Variable** | **Assignment** |
| Start Address | 172.31.6.138 |
| End Address | 172.31.6.250 |
| Subnet Mask | 255.255.255.128 Length: 25 |

Table 0.2 – Park Lane Leeds DHCP Scope

The network access will be subject to a Noddle specific access list providing for connectivity to approved TU UK resources with implicit deny preventing global access to the TU UK network.

It is a project aspiration to extend the current Remote Access VPN solution to provide for an always on VPN implicitly securing the Divestment devices to the TU UK network.

It is also important to note that the initial project delivery will not provide for the Cisco Firepower Threat Defense Anti Malware Protection until such time that the transition to FTD code is completed (scheduled 2019/Q1).

The proposed remote access solution is presented in Figure 2.0 below.

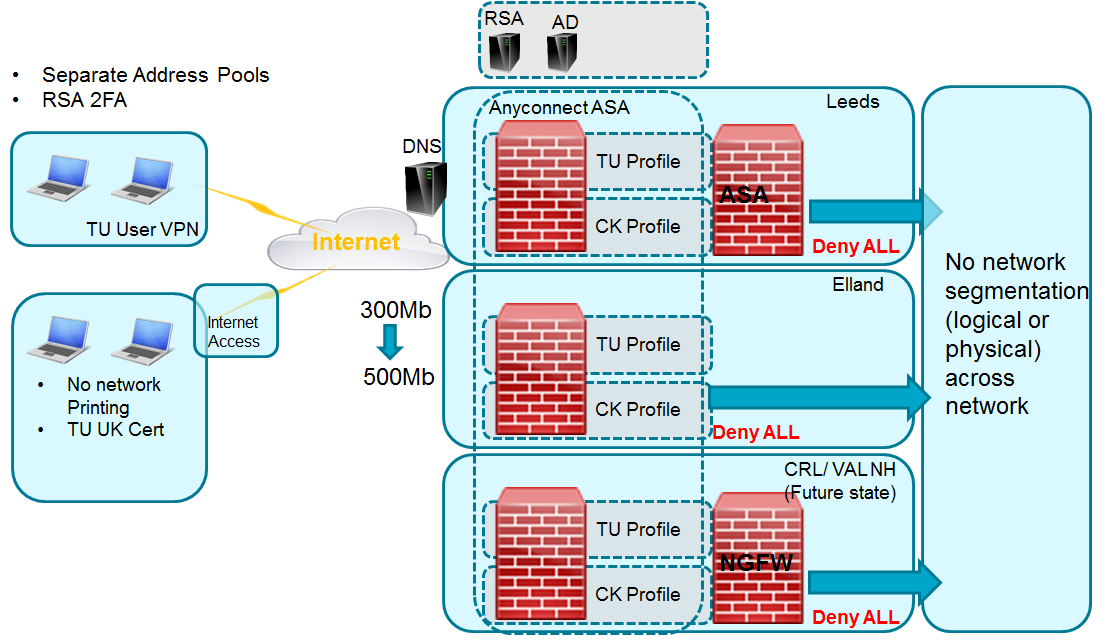


Figure 2.0 – Cisco AnyConnect Client VPN Design

A design objective of the remote access solution is to provide for a like for like user experience which reflects the existing granular access list controls providing Noddle users access to development and production environments from both existing TU UK remote access and PLL wired/wireless LAN.

This design objective will be subject to the DHCP controls available on the Cisco ASA VPN gateway as will be dependent upon issuing a per user or per device fixed lease which in turn will be subject to a granular access list to provide for the required connectivity.

The remote access solution will also provide for access to all resources not currently accessible via the standard TU UK VPN presented in the following table.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Resource** | **URL/Hostname** | **IP Address** | **Port** | **Comment** |
| Build Server | http://pllwinlvbld017.cig.local/nuget | 172.21.164.108 | 3389/tcp |  |
| Service Fabric explorer | https://euacpldv-cluster.consumerplatform.cig.local | 10.53.23.132 | 3389/tcp |  |
| Consumer IaaS Platform (DevTest) | WEUWINDVSQL1  WEUWINDVWEB1  WEUWINDVWEB2  WEUWINDVWEB3 | 172.17.205.170  172.17.205.137  172.17.205.139  172.17.205.136 | 3389/tcp |  |
| Consumer IaaS Platform (Pre-Production) | WEUWINPPSQL1  WEUWINPPSQL2  WEUWINPPWEB1  WEUWINPPWEB2  WEUWINPPWEB3 | 172.17.204.42  172.17.204.43  172.17.204.8  172.17.204.7  172.17.204.6 | 3389/tcp |  |
| Live Noddle Database | TBC | TBC | 3389/tcp | SQL Server Management Studio |

Table 1.0 – Noddle Systems/Environment Access

# End user compute

As part of the Noddle divestment employees will be retaining their existing hardware comprising of monitors and docking stations which will be relocated to the new Office Premises once available.

In accordance with the design decision and security requirements each divesting Noddle Employee will be provided with a re-furbished TU UK Windows 7 build to mitigate TU UK data leakage due to residual data assets located on local hard drives.

The new devices will be TU UK standard Windows 7 builds inclusive of the current machine certificate that is used to authenticate to the remote access solution.

A new Active Directory Security group will be created including all new Noddle user accounts used to authorize each account to the new remote access profile differentiating the Noddle users from standard TU UK remote workers.

The new laptops will support either wired or wireless connectivity to the new Office facilities with local internet access providing for transport to the TU UK provided VPN Concentrators located in Park Lane and Elland.

The current Noddle devices comprise of 44 laptops and PCs presented as follows.

* 20x standard laptops
* 8x developer laptops
* 7x developer desktop PCs
* 5x standard desktop PCs
* 4x WFH laptops

The desktop PCs are used for development purposes and leveraged as jump hosts for remote workers as the current TU UK remote access does not provide for direct connectivity to Noddle development environments.

Rather than rebuild the desktop PCs and expect the Noddle team to vacate Park Lane with both a PC and laptop a design decision has been made to replace users with both Laptop and PCs with a single developer grade laptop as this will minimize the number of devices in the new office premise (1x TU UK and 1x Newcastle device).

## Microsoft Windows 8

A requirement for certain Noddle users running Windows 8 has been identified to maintain access to Microsoft Azure resources and client applications that are not compatible with Current TU UK Windows 7 standard corporate build e.g. SQL 2016.

It is proposed that this requirement is met with the TU UK Windows 7 build with client specific patches where appropriate.

## Security Controls

Client level security controls will be applied to the new Noddle Windows 7 build that will secure the Divestment machines to least privileges whilst permitting the Noddle team to perform their respective job functions business as usual.

The controls that will be delivered on the Noddle devices are summarised as follows.

* No Mapped Personal / Shared Drives
* Forcepoint Proxy enforcement restricting direct internet access outside of the VPN (McAfee)
* Active Directory blocking for WIFI networks located in Park Lane

# microsoft office 365 & collaboration

The Solution supporting the delivery and separation of the Microsoft Office & Collaboration services is presented as follows.

* Delivery of a native, non-object synchronized Microsoft Azure AD instance with conditional access orientated multi factor challenge.
* Delivery of a new Microsoft Office 365 tenant, connected to that native non-synchronized Azure AD instance for the following core collaboration services;

1. Exchange Online
2. SharePoint Online
3. Skype for Business Online

* Leverage the existing TU UK Symantec. Cloud infrastructure for application of security policies pertaining to DLP, Anti-Spam and Anti-Malware but configure the inbound routing to point email for the divested domains to the new tenant
* Leverage the existing TU UK Public DNS registrar for public name resolution services.
* Leverage a transition service in the run up to migration cut over to enable pausing of mail queues and therefore, ensuring no data is lost during the cut over activity.

The new Microsoft O365 Tenant and Office and Collaboration solution is presented in Figure 3.0 below.

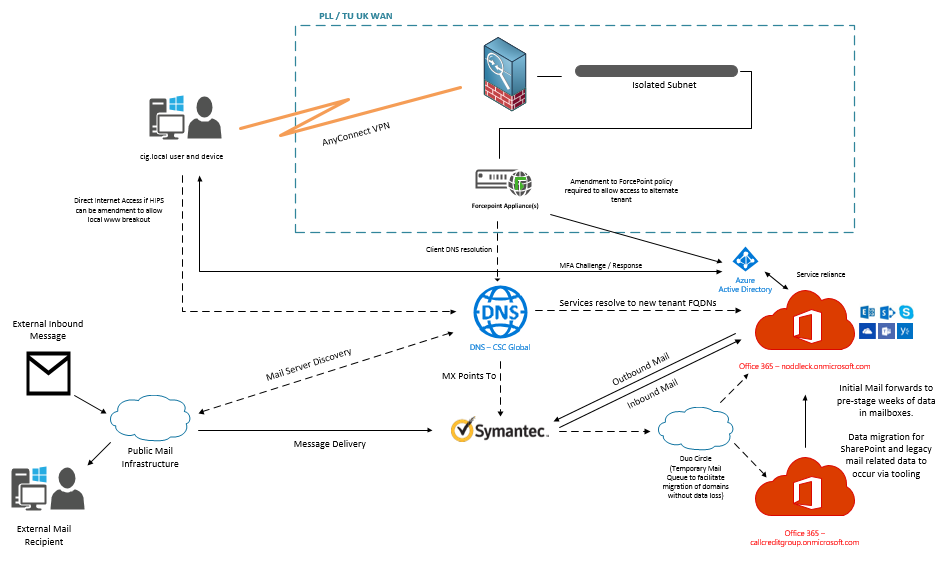


Figure 3.0 – Microsoft Office & Collaboration Design

## Domains and configuration

The following table presents the requirements for the Tenant and Domain names required to be assigned as the Primary email address for all objects.

|  |  |
| --- | --- |
| **Variable** | **Domain Name** |
| Tenant Name | noddleuk.onmicrosoft.com |
| Domain Name | noddleuk.com |

Table 2.0 – Noddle Tenant Domain Names

The chosen domain name will require resource records for both Email and Skype (MX, CNAME, TXT and SRV).

## Email Hygiene and Routing

The new Tenant will leverage the TU UK Symantec Cloud email hygiene solution and TU UK subscriptions and policies providing for Data Leakage Prevention, Anti-Spam and Anti-Malware protection.

The email routing configuration will be configured as follows.

INBOUND MAIL:

* The domain MX records will point to Symantec Cloud (primary and backup)
* The Symantec Cloud will have inbound routing configuration pointing to the Noddle O365 Tenant

OUTBOUND MAIL:

* Outbound email relay will mail forward to the Symantec Cloud.

## Skype for Business

The provision of Skye for Business will be relocated from the current TU UK On-premise solution to the Skype for Business Online service provided in the new O365 Tenant.

Noddle will not require any desktop telephony provision during the TSA (TU Provided hard or soft phone) or Skype for

Business DDI numbers used for inbound and outbound calling.

Therefore, Noddle will continue to use Skype for Business minus DDI for internal collaboration (and TU provided mobile phone as required).

## Intune

The existing Noddle corporate mobiles will be wiped with the Intune Mobile Device Management Software and provided with a new Intune policy providing access to the new O365 Tenant.

## Multi factor authentication

The desktop delivery will leverage the standard TU UK Windows 7 build image and Active Directory which currently provides access to the existing TU UK O365 Tenant via Microsoft Azure conditional access which authenticates each corporate device based upon domain membership with TU UK Corporate Active Directory domain CIG. LOCAL.

Microsoft Azure Conditional Access will not allow a device/domain member to join more than one Microsoft Office 365 Tenant which therefore precludes this control from the new Noddle Tenant which will be in turn accessed from the TU UK corporate Windows 7 build.

Consideration has been given to securing the Noddle Tenant access with alternate controls using Microsoft Multifactor Authentication (MFA).

The implementation of MFA will enforce the requirement for users to authenticate both with their hosted Azure AD user account e.g. [first.last@noddleuk.onmicrosoft.com](mailto:first.last@noddleuk.onmicrosoft.com) and then a second factor from the chosen token method comprising of the following.

1. Phone Call
2. Text Message
3. Push Notification

The user experience would then be subject to the session lifetime between authentication requests which is configurable to meet with the security requirement e.g. 2,4,8,24 hours.

The Conditional Access proposal also includes a second condition which requires the connection to be from a pre-defined location / IP Address which ensures the request is from a legitimate TU UK location.

However, concerns regarding the multifactor user experience, overhead and requirement for a corporate mobile phone which is not currently assigned to all employees have ruled out this additional security control.

It is therefore proposed that the conditional access solution is simplified with defined TU UK locations providing for Internet breakout (presently Park Lane and Elland).

# Microsoft Active Directory

The Active Directory solution will adhere to the TU UK Access Control Policy which mandates internal movers are re-provisioned as new starters, with all previous access removed.

The Active Directory Solution will deliver the TSA objective as follows.

1. Block access to Park Lane Wireless Networks
2. Authorise Noddle users onto the new VPN profile
3. Provide a new user account for each Noddle Employe
4. Provide new Securuity Groups for access to approved TU UK resources.
5. Apply the existing TU UK machine certificate to validate the TU UK device
6. Subject the user to a Noddle VPN profile via membership of a new Active Directory Group ‘CIG.VPN.Noddle’ and Organisational Unit.

## Group Membership

The continued access to Noddle resources located in the TU UK domain shall be maintained via Active Directory group membership.

To solution required to adhere to the TU UK Access Control Policy will be as follows.

* Creation of a new Divestment Organizational Unit (new Container for Newcastle and Future Divestments)
* Creation of a New Organizational Unit for Noddle Employees
* Creation of a New Organizational Unit for new Noddle Laptops
* Creation of New Organizational Unit for Noddle Security Groups
* Creation of New accounts for each Noddle Employee prefixed to differentiate the user e.g. CIG.LOCAL\ndl\_firstlast

The associated Active Directory Groups that provide existing user authorization for Noddle users to internal TU UK systems will be subject to a security audit and mapping to each new user account and new Noddle Specific Security Group on a per business need basis.

The following Noddle roles have been identified which will be compared to sample users to determine the new group memberships required to support the divestment.

1. CST (Customer Service Team) => **ndl\_testusercus**
2. Delivery Manager => **ndl\_testuserdmg**
3. Developer = > **ndl\_testuserdev**
4. Tester => **ndl\_testusertst**
5. Product Owner => **ndl\_testuserpdo**
6. Standard Users => **ndl\_testuserstd**
7. Managing Director=> **ndl\_testusermgd**
8. Operations => **ndl\_testuserops**

The segregation of the Noddle business with within the existing TU UK Active Directory is presented in Figure 4.0 below.

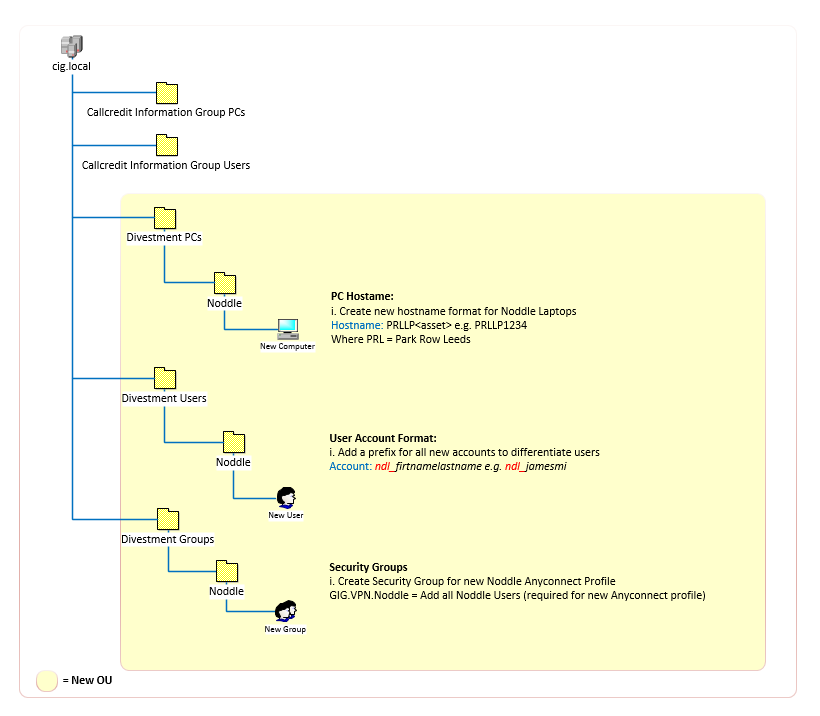


Figure 4.0 – CIG.LOCAL Active Directory Design

## Group Policy

The Active Directory solution will adopt all existing TU UK Group Policies linked to both Computer and User Organisational Units presented in Figure 4.0.

Any Noddle specific policies will be applied via Group Policy Object to either Noddle PC or User containers whereas any Divestment specific policies will be applied at the Divestment Object level e.g. Divestment specific policy to block Park Lane WIFI. Likewise, for any domain or sub domain level policies that are not applicable those policies will be removed via inheritance blocking at either Divestment, Noddle PC or User Organisational Unit levels.

A summary of the initial Group Policy Requirements is presented in the table below.

|  |  |  |
| --- | --- | --- |
| **OU** | **Global Inheritance** | **Container Specific GPO Requirements** |
| ou=Noddle,ou=Divestment PCs,dc=cig,dc=local | Yes | Add Noddle Specific Policy to Block PLL WIFI / SSID |
| ou=Noddle,ou=Divestment Users, dc=cig,dc=local | Yes |  |

Table 3.0 – Group Policy Requirements

# USER EXPerience

## User Accounts

All new Noddle user accounts will be created in a designated OU relating to the Noddle Divestment as indicated below:

**cig.local\Divestment Users\Noddle Users e.g. ndl\_firstlast**

The User Principle Name for each user will follow the standard format albeit with prefix ‘ndl\_’ required to differentiate the users existing UPN e.g. ndl\_firstname.lastname@cig.local,

The pre-Windows 2000 name convention will be, with prefix ‘ndl\_’ required to differentiate the users SAM account e.g. ndl\_<First Name><Last Initial>.

|  |  |
| --- | --- |
| **User Account** | **Format** |
| SAM account | ndl\_firstlast |
| User Principal Name | ndl\_firstname.lastname@cig.local |

Table 4.0 – CIG.LOCAL User Account Format

All user accounts will ***NOT*** require the ‘Azure\_Sync’ parameter adding to the ‘adminDescription’ attribute to ensure synchronisation with Azure Active Directory is not conducted.

## User Devices & Desktop Build

The divestment principle of ‘equivalence’ will be applied to the re-provision of the new hardware to be assigned to each user in terms of the make, model and capacity of their existing laptop / PC e.g. CPU, RAM and HDD.

## Internet Access

Internet access for Noddle users will breakout through TU UK Forcepoint proxy solution currently hosted in Park Lane. This will ensure a common approach is followed for controlled access, as well as enforcing DLP and other security policies.

A McAfee HIPS policy running locally on the client machine will force internet connectivity via ForcePoint which means the user will need to be connected to the VPN to access Internet resources (with exceptions configured for the VPN URL e.g. vpn.callcreditgroup.com).

## User Applications

The following list contains the standard applications required by Noddle staff. Additional applications and systems not covered by this list will be implemented on a case-by-case basis.

|  |  |  |
| --- | --- | --- |
| **Application / Shortcut** | **Path/URL** | **Credentials**  **for Access** |
| Microsoft Word 2016 | Local Path | N/A |
| Microsoft Excel 2016 | Local Path | N/A |
| Microsoft PowerPoint 2016 | Local Path | N/A |
| Microsoft Outlook 2016 | Local Path | AD  noddleuk.onmicrosoft.com |
| Skype for Business 2016 | Local Path | AD  noddleuk.onmicrosoft.com |
| Office365 Portal | <https://login.microsoftonline.com/> | AD  noddleuk.onmicrosoft.com |
| SharePoint on-line | <https://noddleuk.sharepoint.com/> | AD  noddleuk.onmicrosoft.com |
| Intranet | <http://thehub.cig.local/Pages/Home.aspx> | AD  cig.local |
| CORA | <https://eced.fs.em2.oraclecloud.com/homePage/faces/FuseWelcome>? | CORA |
| eLearning Zone | <https://elearningzone.callcredit.co.uk/login/index.php> | eLearning |
| Benefits for People Like You | <https://www.benefitsforpeoplelikeyou.com/CallCredit/Login.aspx?TargetUrl=%2fCallCredit%2f> | BFPLY |
| BarnOwl | <http://cigpllsql10/Voting/default.aspx> |  |
| Concur | <https://www.concursolutions.com> |  |
| Service Request System (VSM) | <http://cigpllvsm01/VSM9_Live/ServiceManager.aspx?Lite> | AD  cig.local |

Table 5.0 – Noddle Application Access Requirements

It is important to highlight that users will be required to login to the desktop with their new SAM (CIG.LOCAL\ndl\_firstlast) or UPN ([ndl\_first.last@cig.local](mailto:ndl_first.last@cig.local)). All subsequent access to applications will then require either System, Tenant or CIG.LOCAL specific Active Directory credentials as required.

A full list of applications that will be required during the Transitional Services Agreement can be found on the project SharePoint ([R5.](https://callcreditgroup.sharepoint.com/:x:/r/coo/etd/Project%20%20Newcastle/Access%20requirements.xlsx?d=wb64f65d1cb434f50b7db053319716325&csf=1&e=iDffpw))

## Cisco Anyconnect

A new Cisco AnyConnect client and XML profile will be deployed to all Newcastle devices to present the user with the required VPN connectivity to the TU UK network.

Users will need to associate their new CIG user account with a new RSA PIN to authenticate with the service using the [RSA Self Service Console](https://valaplcsrsa001.cig.local:7004/console-selfservice/SelfService.do).

## Email

User email will be provided from the new Office 365 tenant provide each user with the address format as follow.

|  |  |
| --- | --- |
| **Noddle O365 Tenant** | **Format** |
| Login | firstname.lastname@noddleuk.onmicrosoft.com |
| Initial Email Address | firstname.lastname@noddleuk.onmicrosoft.com |
| Primary Email Address  (Post Migration of Email Domain ‘noddle.co.uk’) | [firstname.lastname@noddle.co.uk](mailto:firstname.lastname@noddle.co.uk) |

Table 6.0 – Noddle O365 Tenant User Account Format

It is important to note that customer services mailboxes will be assigned the Primary email address ‘@noddle.co.uk’ following the transfer of the domain from the existing TU UK O365 Tenant.

## Sharepoint

Subject to the data transfer policy all identified SharePoint documents and any data residing on internal on-premise file shares will be synchronized with the new Tenant.

## ONEDRIVE for business

Subject to the data transfer policy all identified personal SharePoint libraries and any data residing on internal TU UK home drives will be synchronized with the new Tenant.

## Cryoserver

Subject to the data transfer policy all identified email archives resident in Cryoserver shall be exported in PST format and provided to each user.

# data Migration

## Policy

The initial project delivery will provide for the new Tenant, licensing and creation of new user accounts and active directory groups to allow for parallel running between TU UK and Noddle O365 Tenants.

The Tenant will then be populated with Data at numerous levels which align to the contractual requirements relating to the transfer of data. The table below presents the data migration assets and the respective archive period and security policy requirements that must be adhered.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **TU UK Tenant** | | | **Noddle Tenant** |
| **callcreditgroup.com** | | | **noddleuk.onmicrosoft.com** |
| **Transfer Policy  [Y/N]** | **Archive CryoServer** | **Security Control** | **Sync Method** |
| **Customer Service Mailbox** |  |  |  |  |
| Office 365 | 30 Days | 6 Years | n/a | BitTitan Migration Wiz |
|  |  |  |  |  |
| **Personal Mailbox** |  |  |  |  |
| Office 365 | 24 Months | n/a | TBC | BitTitan Migration Wiz |
|  |  |  |  |  |
| **Personal Data** |  |  |  |  |
| One Drive for Business | TBC | n/a | Veronis DLP | TBC |
| Home Drives | TBC | n/a | Veronis DLP |  |
|  |  |  |  |  |
| **Shared Data** |  |  |  |  |
| SharePoint Libraries | TBC | n/a | n/a | TBC |
| On Premise Shared Folders | TBC | n/a | n/a | TBC |
|  |  |  |  |  |

Table 7.0 – Data Migration Policy

## Process

All Noddle User Personal and Shared Drives will be subject to DLP inspection (Veronis) before being transferred to TU UK O365 One Drive for Business ready for Migration.

## Dual Running

As specified in TSA Schedule EUIT004 the Noddle consumer will be provided with dual access to current TU UK and new Noddle Tenant for up to a period of 6 weeks from the completion date.

The user experience aligned to dual running will be managed via 2x Outlook client profiles required for each Tenant during the 6-week transition period.

Once the user’s mailbox is migrated to the new Tenant access to the TU UK Tenant mailbox will be disabled and user access to Noddle O365 only accessible via the new Tenant profile.

# Software LICENSING

The following software components will be required to support the delivery and data migration required to support the Noddle Divestment.

|  |  |  |  |
| --- | --- | --- | --- |
| **Qty** | **Description** | **Unit Cost** | **Total Cost** |
| 58 | Office 365 Enterprise E3 licenses with EMS E3 | TBC | TBC |
| 1 | Domain Registration (noddleuk.com) | TBC | TBC |
| 1 | Duo Circle Email Forwarding Subscription (Mail Migration) | TBC | TBC |
| 1 | BitTitan Migration Wiz (Mail Migration) | TBC | TBC |
|  |  |  |  |

Table 7.0 – Software Licensing

# Design Decisions & Issues Backlog

## Design Decisions

|  |  |  |
| --- | --- | --- |
| **Ref** | **Design Point/Options** | **Decision & Justification** |
| 1. DP1. | All divesting users will be provided with a new TU UK Windows 7 desktop build | The decision to deliver a new build to the Noddle employees is to mitigate any data leakage resident on local hard drives. |
| 1. DP2. | The connectivity solution will be TU UK standard remote access (Cisco AnyConnect Full Tunnel VPN) | There will be no exception to Full Tunnel e.g. split tunnel required for local printing. |
|  | The connectivity solution will whitelist access to approved TU UK resources | Noddle RAS users will be differentiated with a new user subnet and whitelisted to required CIG resources. |
| 1. DP3. | All divesting users will receive a new Active Directory account | This control will be subject to Proof of Concept and user experience reflecting the device and User two factor authentication. |
| 1. DP4. | All divesting users will receive new Active Directory Groups controlling access to TU UK resources | To provide for clear separation the Noddle users will be provided with a new CIG.LOCAL user account and provided with Group memberships relative to business need. |
| 1. DP5. | All divesting users with both Laptop and PCs will received a single developer specification Laptop | This decision will minimize the number of devices in the new office premise (1x TU UK and 1x Newcastle device). |

## Issues Backlog

|  |  |  |
| --- | --- | --- |
| **Ref** | **Description** | **Resolve** |
|  |  |  |

## Outstanding Questions Log

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Question** | **Assigned** | **Response(s)** |
|  |  |  |  |

## Post-Design Points/Activities

The following table lists any points raised as part of the design process that need to be considered as either a future phase of change in architecture that relates to this solution, or for information that may relate to other systems or projects.

|  |  |  |
| --- | --- | --- |
| **Ref** | **Point** | **Assigned (if relevant)** |
|  |  |  |

# Appendix A Project Delivery sequence

