Data Communications Company

DCC Internet Access Policy

Version: 1.0
Date: 05/03/2026
DCC Public

Table of Contents

1. Introduction

This document is the DCC Internet Access Policy, which is established and maintained in accordance with Clause 1.4A of the Self-Service Interface Code of Connection.

This document lays out the eligibility and technical requirements for access to the DCC Service Management System (DSMS) Self Service Interface (SSI).

It will also detail aspects of the access and authentication process that are applicable to the following two groups:

- Users accessing the SSI via public internet; and
- Users accessing the SSI via a DCC Gateway.

Note on terminology: the components of the DSMS solution that are relevant to this document are the following.

- Entra: Microsoft provisioned DCC Identity Provider Service. This is an extensible identity management capability and is part of the DCC future vision for Single Sign On (SSO), meaning that setting up the DCC Identity Provider Service from day one will enable future benefits as other systems are brought within the scope of this identity service. The use of this platform is optional (due to connectivity requirements described later in this document some parties may not be able to support DCC Identity Provider Service and therefore have the option to use local ServiceNow user accounts). Note: at this time only ITSM and OMS will be subject to the Single Sign On service.
- ServiceNow: core ITSM / DSMS / OMS platform. Provision of the SSI is via the ServiceNow portal / UI.

Document control

Revision history

Revision date	Summary of changes	Changes marked	Version number
07/07/2025	Draft	No	0.1
11/07/2025	Updated following peer review	No	0.2
24/07/2025	Updated following DESNZ review	Yes	0.3
15/09/2025	Updated following Response to Consultation	Yes	0.4
19/09/2025	Updated to reflect voice authentication as the Entra back up method	Yes	0.5

2. Accessing the SSI via the internet

2.1. Eligibility

User organisations without a DCC Gateway Connection who require access to SSI will be eligible to set up a connection via public internet. User organisations with legitimate use cases that do have a DCC Gateway connection may also be eligible to set up a connection via public internet. This will be managed by DCC on a case-by-case basis.

DCC preference is for user organisations to access the SSI via a private network (i.e. the DCC Gateway). The rationale for this position is security hardening and principle of secure by design: access via a private network is more secure than access via public internet, therefore if access via a private network is possible this should be the default position for User access.

Please note that the security posture for internet connectivity has been deemed sufficient by the Security Sub Committee (SSC), so this is not to suggest that internet connectivity with the controls proposed is insecure, but that a private network is more secure. This will be subject to regular re-assessment.

These considerations apply to both the UIT and Production environments.

2.2. Technical requirements

Below are the technical requirements for accessing the SSI via the internet

- Access from a fixed range of IP addresses
    - This will be configured across the ServiceNow UIT and Production instances to ensure that only authorised organisations are able to access the relevant ServiceNow instance via the internet. This will require that each organisation is connecting from a known and trusted network (e.g. a corporate network) with a known IP address (or range of IP addresses). All other access requests will be denied (e.g. a user working from home if not accessing via the corporate network; dynamic IP addresses outside of a range).
- Protocol
    - Use of a secure protocol (namely HTTPS). If HTTP is used this will automatically be redirected to HTTPS.
- Custom URLs.
    - Custom URLs will be configured for the Users requiring access to FSM via the Internet to use when accessing the different FSM ServiceNow instances (UIT and Production). These have not been configured at the time of writing but will be shared with Users as part of cutover preparation / onboarding.

Security controls and hardening within ServiceNow will be exactly as per connectivity via the DCC Gateway private network. ServiceNow maintains many global and regional security and privacy certifications including the internationally recognized ISO 27001, ISO 27017, ISO 27018, and ISO 27701.

3. Authenticating to SSI via the DCC Identity Provider Service

3.1. Requirement to use MFA

For users who utilise the DCC Identity Provider Service, Multi Factor Authentication (MFA) will be used for authentication (i.e. verification of the user's identity). This will be the case for access via public internet and access via a DCC Gateway Connection.

The user will be assigned a one-time password at the point of cutover / onboarding. Once they login, they will be prompted to set up one of the following authentication factors as preferred (detailed in subsequent sections). This can be changed at any time.

- Authenticator application
- Voice authentication

An authentication session will last for nine hours before re-authentication is required.

3.2. MFA options

This section sets out the details around the MFA options that the DCC will make available to users. Authenticator applications are considered the most robust measure and therefore are the DCC's recommendation. However, the other methods are available to give flexibility to Users.

3.2.1. Authenticator applications

This subsection details the MFA applications available to users for logging into FSM.

- The DCC recommend Microsoft Authenticator due to the close and extensively proven integration with Microsoft Entra.
- Users are free to use their preferred authenticator apps (such as Google Authenticator).
- The most recent version of any authenticator application should be used.
- Please note that **all** authenticator applications sit outside the DCC estate, any support will be provided on a reasonable endeavours' basis, and support will ultimately sit with the provider of the application.

3.2.2. Alternative methods

This subsection sets out the routes available to users to obtain a one-time password for logging in to FSM.

3.2.2.1. Voice Authentication

A call will be placed to a contact number configured at the point of the user credentials being created, at which point the user will press a button as requested to authenticate.

3.3. Microsoft domain connectivity requirements

As a SaaS product, Entra has a lot of distributed resources that it manages workload across, and therefore authentication traffic could be routed to several different endpoints. This means that each endpoint attempting to authenticate against Entra will require a route to reach it. Therefore to use the Entra solution internet connectivity from Users must be available to the following URL domains:

- login.live.com
- login.microsoft.com
- login.microsoftonline.com
- Login.windows.net
- sts.windows.net

Where opening routes to these end points via the internet is not possible Users have the option to use a local ServiceNow user identity. This will limit the ability for Users to take advantage of potential future

extensions to the SSO capability delivered by the DCC Identity Provider Service (although Users will have the option to move from the local ServiceNow identity to the DCC Identity Provider Service in the future).

4. Authenticating to SSI via the local ServiceNow user identity

4.1. Requirement to use MFA

For users who use a local ServiceNow user identity, MFA will be used for authentication (i.e. verification of the user's identity). This will be the case for access via public internet and access via the DCC gateway.

The user will be assigned a onetime password at the point of cutover / onboarding. Once they login they will be prompted to set up one of the following authentication factors as preferred (detailed in subsequent sections). This can be changed at any time.

- Authenticator application
- Email one time password (OTP)

An authentication session will last for nine hours before re-authentication is required (except for e-mail OTP which will be required for each login).

4.2. MFA options

This section sets out the details around the MFA options that the DCC will make available to users.

4.2.1. Authenticator applications

This subsection details the MFA applications available to users for logging into FSM.

- The DCC recommend Microsoft Authenticator due to the close and extensively proven integration with Microsoft Entra.
- Users are free to use their preferred authenticator apps (such as Google Authenticator).
- The most recent version of any authenticator application should be used.
- Please note that **all** authenticator applications sit outside the DCC estate, any support will be provided on a reasonable endeavours' basis, and support will ultimately sit with the provider of the application.

4.2.2. Single-use codes

This subsection sets out the routes available to users to obtain a one-time password for logging in to ServiceNow.

4.2.2.1. Received via email

A one-time password per authentication request will be emailed to the user at the email address they configured at the point of their credentials being created. This must be a corporate email address to align with security controls between DCC and Users.

5. Internet Browser compatibility

5.1. Supported browser principles

Below are the browsers that the ServiceNow UI supports.

Browser	Supported
Chrome	Latest public release of the browser, and the two previous releases
Firefox and Firefox ESR	Latest public release of Firefox and Firefox ESR, and the two previous releases
Internet Explorer	Not supported
Microsoft Edge Chromium	Latest public release of the browser, and the two previous releases
Safari	Safari 12.0 and newer
Tablet Mobile	Supported
Phone Mobile*	Not supported* **Mobile phone browsers do not support the desktop version of the UI. Instead, mobile browsers use the mobile UI. Not in day one scope for the replacement DSMS (FSM)*