Queensland Government Enterprise Architecture

Collaborative workspace

Wired and wireless network access control guideline

Final

December 2017

V1.0.0

PUBLIC

Document details

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1. **Security classification** | 1. PUBLIC | | | | | |
| 1. **Date of review of security classification** | 1. May 2017 | | | | | |
| 1. **Authority** | 1. Queensland Government Chief Information Officer | | | | | |
| 1. **Author** | 1. Strategic Transformation | | | | | |
| 1. **Documentation status** |  | 1. Working draft |  | 1. Consultation release | 1. 🗹 | 1. Final version |

Contact for enquiries and proposed changes

All enquiries regarding this document should be directed in the first instance to:

QGCIO  
[rod.muller@qgcio.qld.gov.au](mailto:rod.muller@qgcio.qld.gov.au)

Acknowledgements

This version of the *Wired and wireless network access control guideline* was developed and updated by QGCIO, Strategic Transformation.

Feedback was also received from a number of agencies, which was greatly appreciated.

Copyright

Wired and wireless network access control guideline, Copyright © The State of Queensland (Queensland Government Chief Information Office) 2017

Licence

[](http://creativecommons.org/licenses/by/4.0/)

This work is licensed under a Creative Commons Attribution 4.0 International licence. To view the terms of this licence, visit <http://creativecommons.org/licenses/by/4.0/>. For permissions beyond the scope of this licence, contact [qgcio@qgcio.qld.gov.au](mailto:qgcio@qgcio.qld.gov.au).

To attribute this material, cite the Queensland Government Chief Information Office.

The licence does not apply to any branding or images.

Information security

This document has been security classified using the Queensland Government Information Security Classification Framework (QGISCF) as PUBLIC and will be managed according to the requirements of the QGISCF.

Contents

[1 Introduction 4](#_Toc18916412)

[1.1 Purpose 4](#_Toc18916413)

[1.2 Audience 4](#_Toc18916414)

[1.3 Scope 4](#_Toc18916415)

[2 Mobility enablement 5](#_Toc18916416)

[2.1 Key issue 5](#_Toc18916417)

[2.2 ICTSS.1405A Agency Integration Service guidelines 5](#_Toc18916418)

[2.3 Exemption guidelines 18](#_Toc18916419)

Figures

[Figure 1 – Agency to POP connectivity 6](#_Toc18916420)

[Figure 2 – AutoConfig Service 9](#_Toc18916421)

[Figure 3 – Authentication Settings 10](#_Toc18916422)

[Figure 4 – Authentication tab 10](#_Toc18916423)

[Figure 5 – Network authentication method 11](#_Toc18916424)

[Figure 6 – Settings 11](#_Toc18916425)

[Figure 7 – Certificate properties 12](#_Toc18916426)

[Figure 8 - Advanced settings 13](#_Toc18916427)

[Figure 9 - Authentication mode 13](#_Toc18916428)

[Figure 10 – Setup new network connection 14](#_Toc18916429)

[Figure 11 – Manual connection 14](#_Toc18916430)

[Figure 12 - Network Name 15](#_Toc18916431)

[Figure 13 Change connection settings 15](#_Toc18916432)

[Figure 14 – Connection security 16](#_Toc18916433)

[Figure 15 – Use certificate 17](#_Toc18916434)

[Figure 16 – Authentication mode 17](#_Toc18916435)

Tables

[Table 1 – Example of the 1WS, AIS spreadsheet 7](#_Toc18916436)

[Table 2 CRL Requirements 8](#_Toc18916437)

[Table 3 - CRL Sample spreadsheet 8](#_Toc18916438)

[Table 4 – Sample DNS spreadsheet 8](#_Toc18916439)

# Introduction

To ensure that the delivery of government services underpinned by information technology is collaborative reliable, low risk, cost effective and agile, the Queensland Government will standardise the implementation of inbuilding wired and wireless ICT infrastructure and services in alignment with the QGEA [Collaborative workspace strategy and principles](https://www.qgcio.qld.gov.au/documents/collaborative-workspace-strategy)

The basic architectural principles contained in the strategy are described as follow:

* any person, anywhere, anytime access to services provided by Dimension Data
* a robust security model not focussed on perimeter and edge security, but more so leveraging identity, application security and endpoint controls.
* shared infrastructure (both wired and wireless).
* logical separation where required.
* “as a Service” consumption model.
* architecture to allow for a repeatable deployment model.

## Purpose

This guideline provides information and advice for Queensland Government departments to consider when implementing the policy requirements of the Queensland Government Enterprise Architecture, [Collaborative workspace policy](https://www.qgcio.qld.gov.au/documents/collaborative-workspace-policy). These guidelines assist in complying with mandatory components of the policy and are for information only. While some information communicates other mandatory obligations, which may be relevant in the context of the policy (e.g. compliance to other policies), departments are strongly recommended to further investigate these obligations in light of their own business requirements, and seek expert advice where necessary.

## Audience

This document is primarily intended for solution architects of all Queensland Government departments and internal Queensland Government ICT service providers.

The intent is to supply the agency chief information officers (CIOs) with information of where the wired and wireless network (WWN) service will interface with agency production environments and to give certainty of what is being asked of the agency from a design and integration perspective. It is also designed to give the relevant technical subject matter experts (SMEs) the necessary high level information to complete all the required steps to integrate the agencies ICT systems with the buildings ICT core infrastructure.

## Scope

This document provides an overview of the WWN service that is available to agencies and what underpinning technologies are used to provide the service. Additional information can be obtained from the integrator or the One William Street (1WS) Contract Directorate (Agency Integration Service (AIS) Supporting Services and Agency AIS Configuration Spreadsheet) to provide clarity around what is being requested of agencies to configure their infrastructure to use these services.

Agencies contracting the WWN services under ICTSS.1405A will be provisioned with an end-to-end service model using proven ICT technologies and service providers. The expected benefits of establishing common ICT services and using a consumption-based service model include:

* providing the benefits of common technologies to agencies without the need to invest in the infrastructure or take on the risk of owning and operating the infrastructure
* providing a utility reporting and billing model, enabling agencies to scale costs up and down according to need without being constrained by assets
* increasing standardisation of IT infrastructure across government and reduce duplication
* resulting in a single procurement process rather than each individual agency undertaking their own process
* providing a repeatable model for other multi-floor, multi-agency buildings.

# Mobility enablement

These guidelines will ensure that the “anywhere, anytime and any device” connectivity outlined in the [Collaborative workspace strategy](https://www.qgcio.qld.gov.au/documents/collaborative-workspace-strategy) and principles will deliver seamless and secure access to agency networks throughout government buildings without the need for agency intervention.

The following guidelines will assist agencies implement whole-of-government wired and wireless network mobility enablement for all government tenanted buildings.

## Key issue

To assist the Queensland Government to work more effectively the [Collaborative workspace strategy and principles](https://www.qgcio.qld.gov.au/documents/collaborative-workspace-strategy) outlines a WWN architectural pattern that enables users from any agency the ability to connect either wired or wirelessly in any integrated building and be operational.

Although 1WS has been configured to allow all Queensland Government agencies the ability to “plug in” and connect to their data centre applications and data, unfortunately agency integration into subsequent buildings has not been performed. The result being, agency staff other than the tenants of the subsequent buildings will only have Guest Wi-Fi services available, therefore requiring agency supplied remote access facilities to access applications and data residing in their data centres.

## ICTSS.1405A Agency Integration Service guidelines

Agencies contracting the WWN services under ICTSS.1405A should follow the following Agency Integration Service (AIS) requirements.

### Network Connectivity

There are number of core services that the panel integrator will provide to agencies to access their corporate network and base services. These are:

* Wired and Wireless Networking - the ability to connect to an agency network with admission control based on the use of digital certificates and Public Key Infrastructure.
* Guest Wireless – providing Internet access only for Agency users and guests that do not have the need to connect to agency resources.

The building network should comprise of multiple Virtual Route Forwarding (VRF’s) configurations. These VRF’s are created to segregate agency traffic from other agencies and from the shared services.

The agency home network connects to the agency VRF over the Queensland Government Network (QGN). This is shown below.

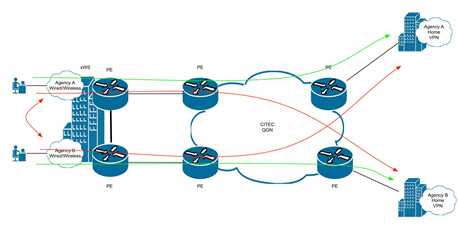


Figure – Agency to POP connectivity

Boarder Gateway Protocol (BGP) is used to connect the POP to the QGN. For redundancy, there may be 2 connections to the QGN.

To configure these connections agencies (via CITEC) will provide 2 x /30 IPv4 subnets to be used for the point to point links as well as an ASN for the QGN network.

The POP network will utilise the same autonomous system number (ASN) across all agency VRF’s within the building. Additional buildings will contain additional ASN’s.

### Agency Firewalls, Building VLAN to Agency Network

Agencies may or may not have firewalls positioned between any integrator provisioned building VLAN and the remainder of their network. Any additional IP address range defined for buildings, both current and future, should be added by agencies to existing firewall rules to ensure the ability for staff to roam from building to building and access all required applications and data.

### IP Addressing:

The integrator and/or agency will need to collect AIS information to integrate each agency into each building complying to the collaborative workspace architectural pattern.

For most agencies, this will include VLAN’s for Wired, Wireless and Voice.

These only need to be small as it is for use by agency staff that are temporarily visiting the site. If an agency is permanently using a site, they should re-assign larger subnets that cater for the number of resident staff.

As an example, an agency could supply the ITSS.1405A panel integrator a /25, broken up as follows:

* /26 – Wireless – 64 devices
* /27 – Wired – 32 devices
* /27 – Voice – 32 devices

However, each agency may have different policies that dictate what they assign.

NB: It would be preferable to collect this information for 10 buildings up front, so agencies are not constantly being requested to provide this information. Additional Tabs of the AIS spreadsheet on the Dimension Data Australia (DDA) FTP site can be leveraged to define additional IP address ranges.

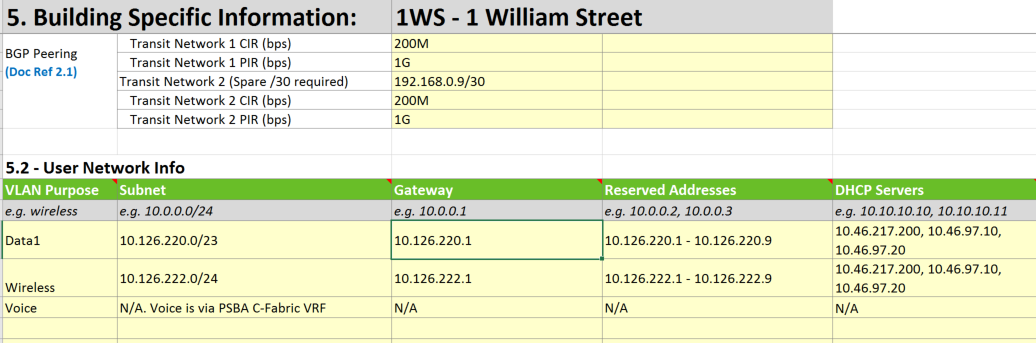


Table – Example of the 1WS, AIS spreadsheet

### Wi-Fi Service Set Identifier (SSID)

The SSID differentiates one WLAN from another, so all access points and all devices attempting to connect to a specific WLAN must use the same SSID to enable effective roaming. As part of the association process, a wireless network interface card (NIC) must have the same SSID as the access point or it will not be permitted to join the network.

In order to provide a consistent naming standard across government agencies should use the following service set identifiers:

* QGov-Corp (connectivity to agency corporate networks from managed devices)
* QGov-CorpGuest (connectivity to filtered guest internet for users with a government identity)
* QGov-Guest (connectivity to filtered guest internet for users without a government identity.

### Certificate Revocation Lists (CRL)

Users connecting to wired and wireless infrastructure in a building will require a digital certificate to identify the user and verify their authorisation to connect to the infrastructure. If an agency has a certificate revocation service exposed on either GovNet or the public Internet, access is required from the identity services to the CRL service to retrieve the list.

The following table describes the agency requirements for this service.

|  |  |  |  |
| --- | --- | --- | --- |
| Service | Service Dependency | Information and Configuration Required from Agency | Information and Configuration Provided by the integrator to Agency |
| CRL | DNS | Agencies need to provide Integrator the full URL of the location where the Certificate Revocation List can be sourced. If the agency CRL listens on a custom port, that port will be required to configure Dimension Data services to retrieve the CRL on that port. If no CRL is offered, no revocation checks can be made on agency certificates. | The integrator will provide to the agencies the source of the request in the agency AIS spreadsheets. |

Table CRL Requirements

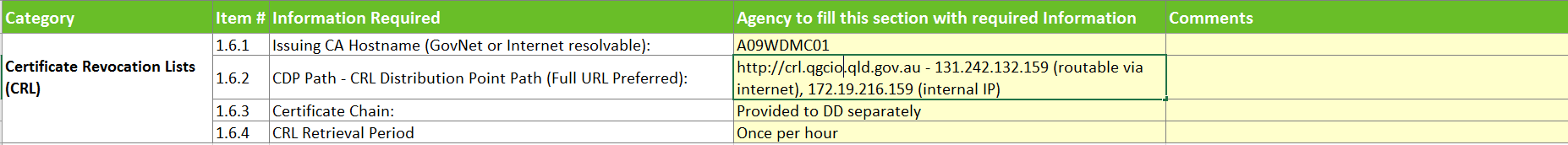


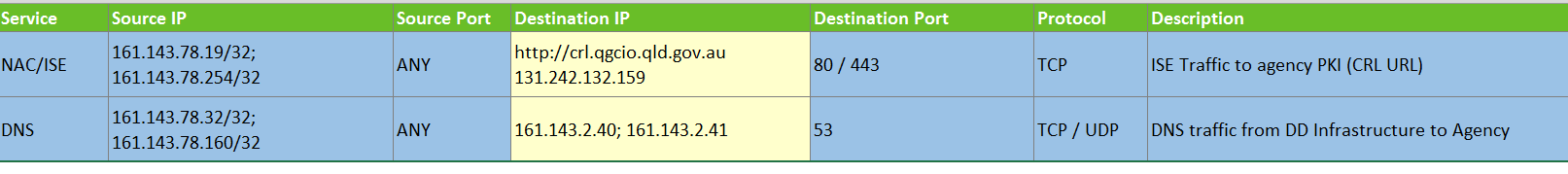
Table - CRL Sample spreadsheet

### DNS Name Resolution

Each agency should perform a conditional forward for the QGAAAD.QLD.GOV.AU domain to the Extranet facing domain name servers that host that domain. Failure to do so will result in Internet facing DNS name resolutions being returned to users, rendering them unable to use Extranet only services.

Agencies who host their own Extranet facing DNS servers (including those whose DNS is handled by a third party, but are still presented on Extranet) should also permit access from QGAAAD.QLD.GOV.AU name servers to their name servers.

The firewall rule requirements for DNS are outlined in the Agency AIS Configuration Spreadsheet example below:



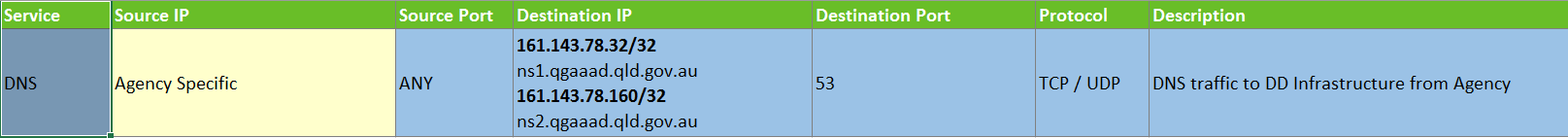


Table – Sample DNS spreadsheet

### 802.1x Certificates

The corporate devices connected to the wired and wireless LAN in any transformed building shall be authenticated using X.509 certificates. The procedure for configuring the Microsoft Windows devices is described below. It is by no means an exhaustive explanation of the topic but it explains how this task can be performed manually. In production, it is expected that each government agency will deploy these configurations via an IT group policy.

Wired and wireless is somewhat different, but they still use the same certificate. In general, the Windows host should have its own unique machine certificate pre-installed prior to beginning with the configurations.

1. Enable the wired AutoConfig service

* By default, Windows does not perform EAP authentication on wired connections. To enable this, start the Windows service called ‘Wired AutoConfig’.
* Launch the services.msc tool and choose the Standard tab, find Wired AutoConfig and start the service.

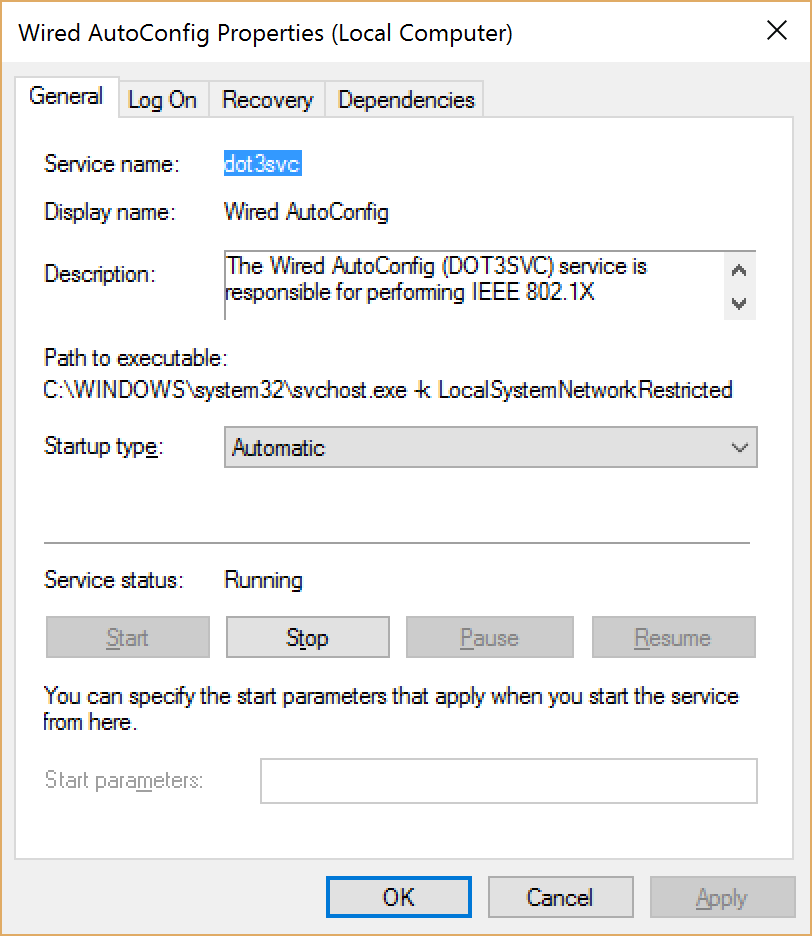


Figure – AutoConfig Service

1. Configure the wired LAN adapter authentication settings

* Once the AutoConfig service is running you will notice a new tab called ‘Authentication’ under the wired LAN adapter properties

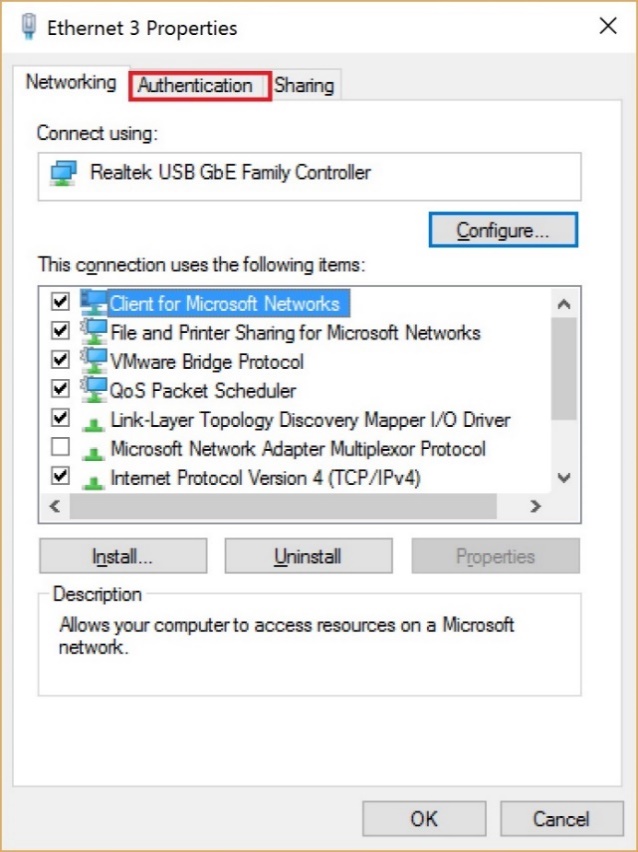


Figure – Authentication Settings

1. Select the Authentication tab

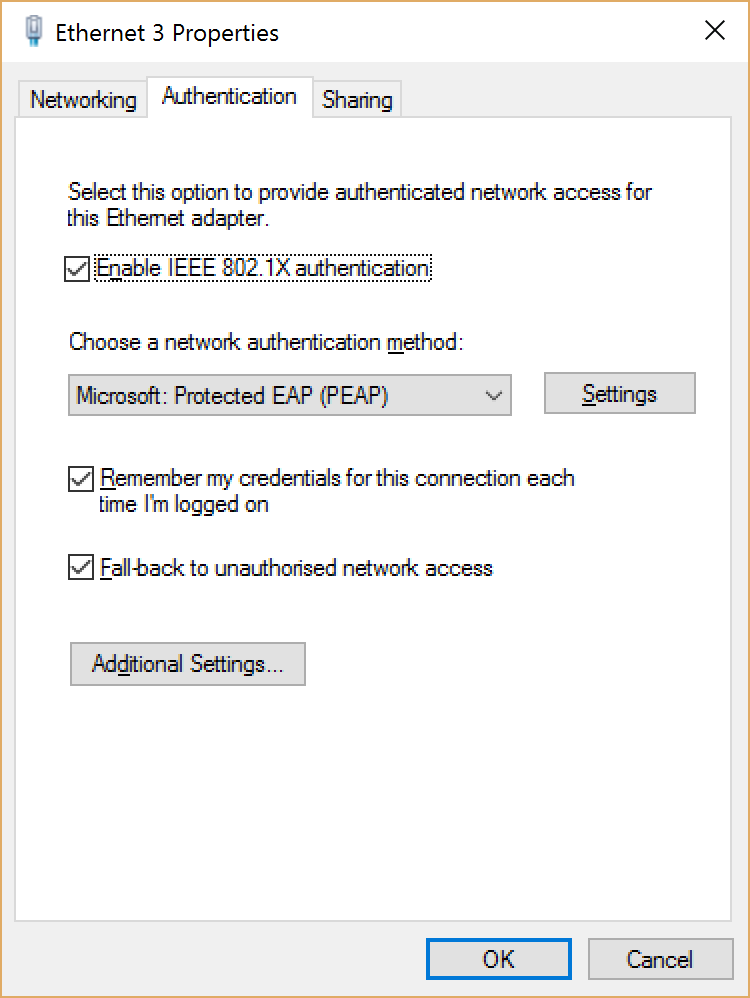


Figure – Authentication tab

1. Amend the network authentication method for certificate based authentication and ensure that the Fall-back check box is in place to allow the adapter to still function normally in non-802.1x environments.

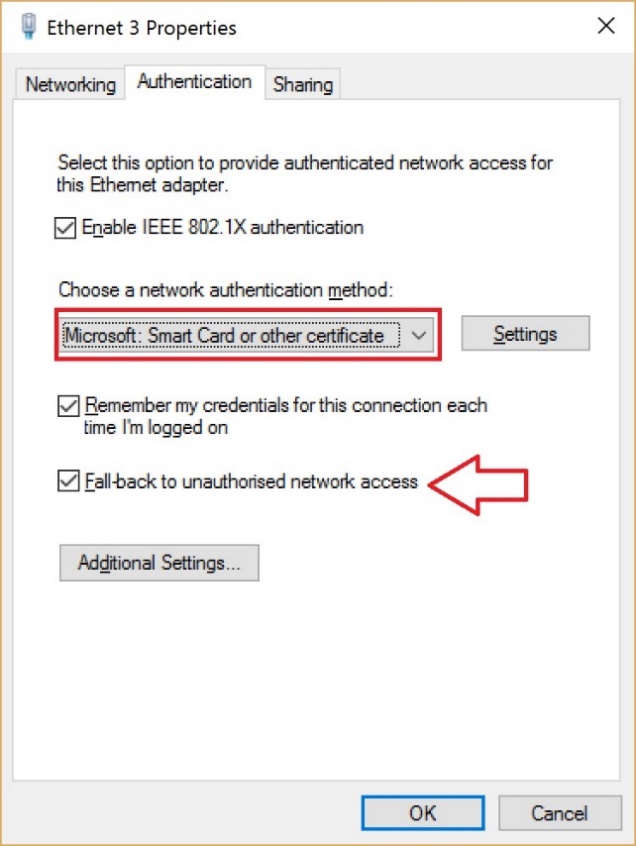


Figure – Network authentication method

1. Click on Settings and the following default settings will be displayed:

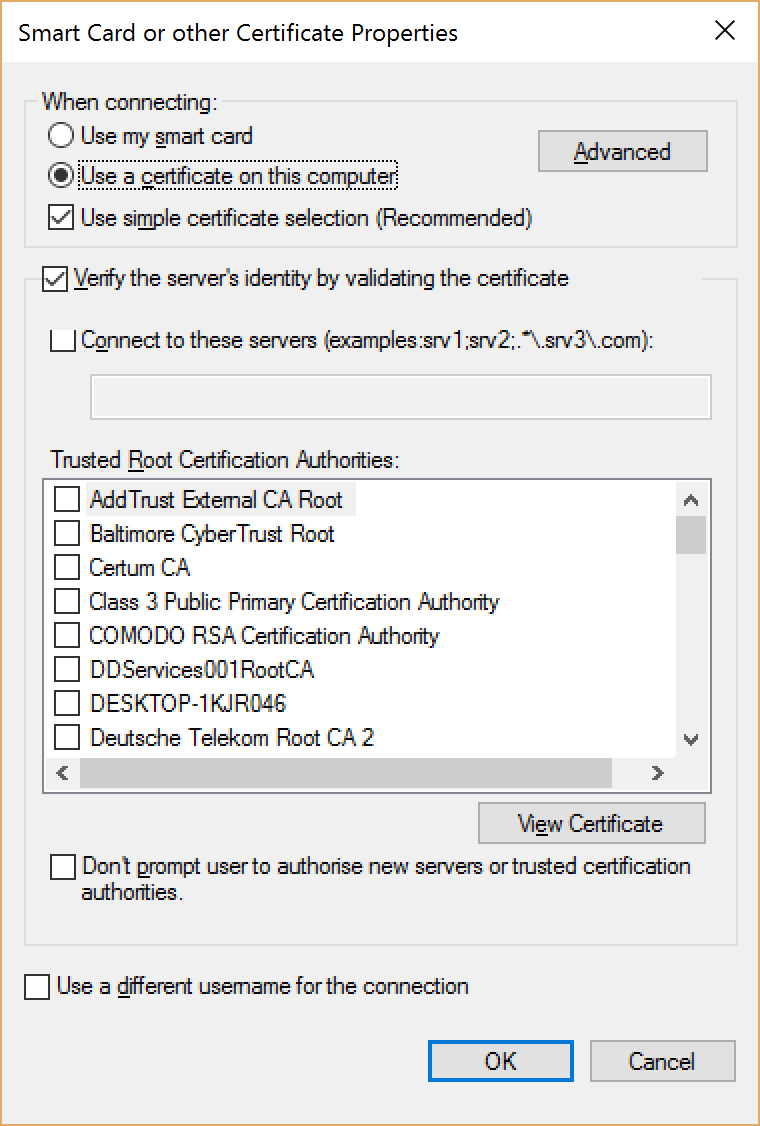


Figure – Settings

1. Configure the following:

* Tick the checkbox to validate the AAA server and enter the domain name ise.qgaaad.qld.gov.au
* Find the Go Daddy Trusted Root Certificate Authority – G2 and check it
* Check the box to avoid getting a confirmation prompt
* Click OK

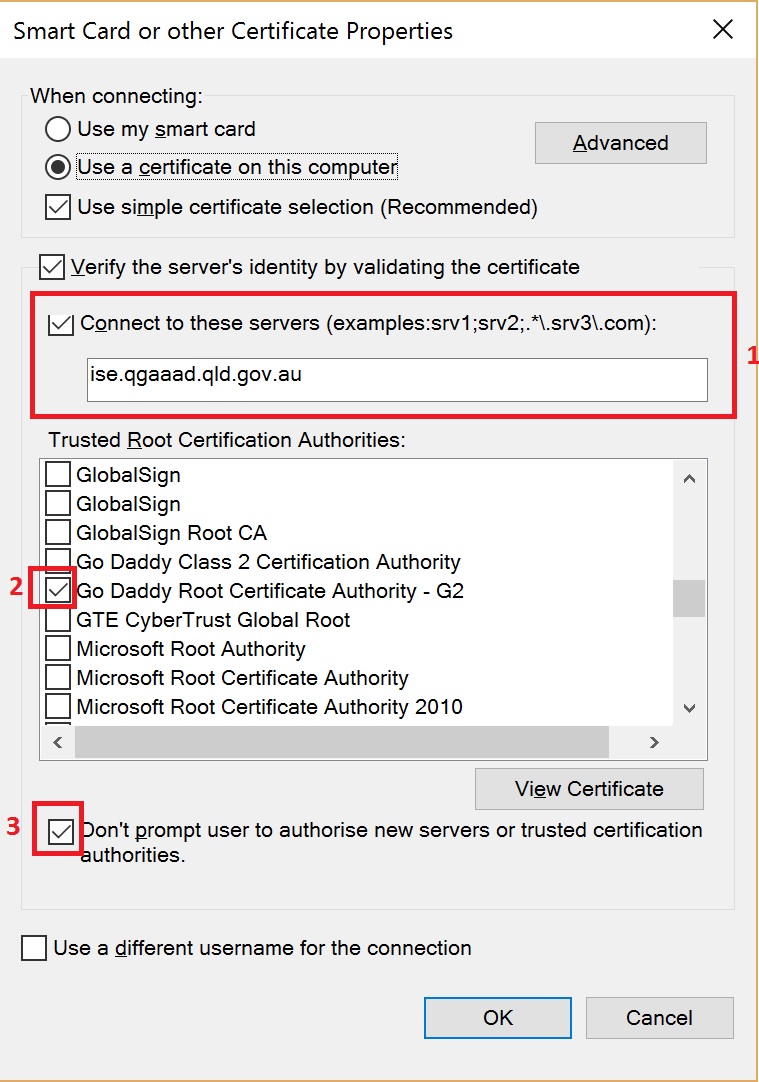


Figure – Certificate properties

1. Click on Additional Settings and you will see the defaults

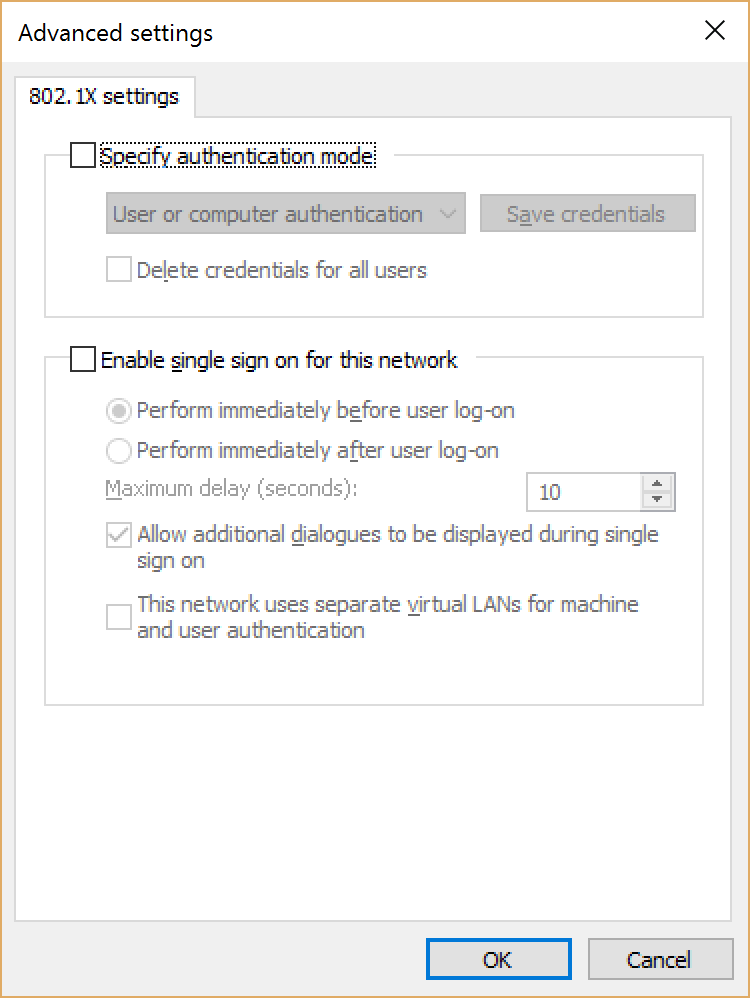


Figure - Advanced settings

1. Put a check in the Specify authentication mode box and then choose Computer Authentication.

* Click OK. Click OK to close the final window.

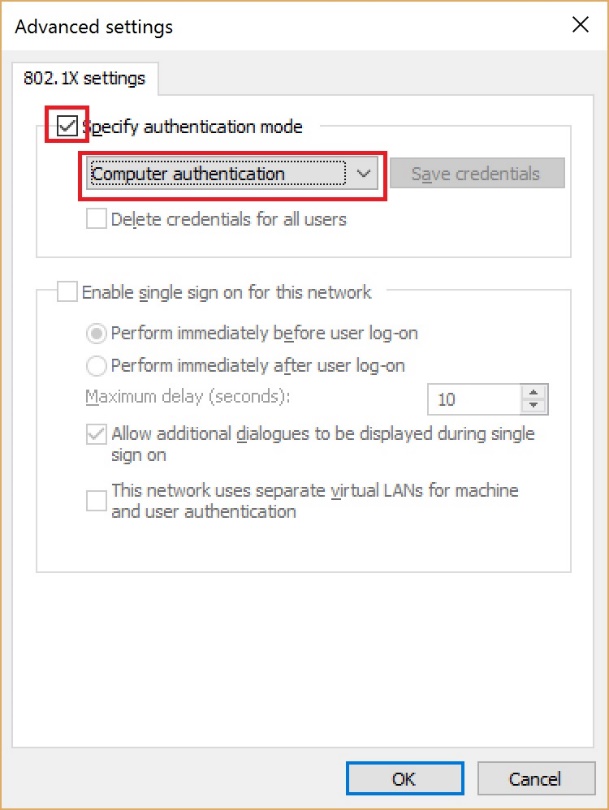


Figure - Authentication mode

### Configuration for wireless connection (Wi-Fi adapter)

1. There should be no need to enable any 802.1 Windows service for Wi-Fi since it is already enabled by default.
2. However, you will need to configure the EAP supplicant for your wireless adapter.
3. Setting up the wireless EAP supplicant
   * + 1. Launch the Control Panel and Set up a new connection or network

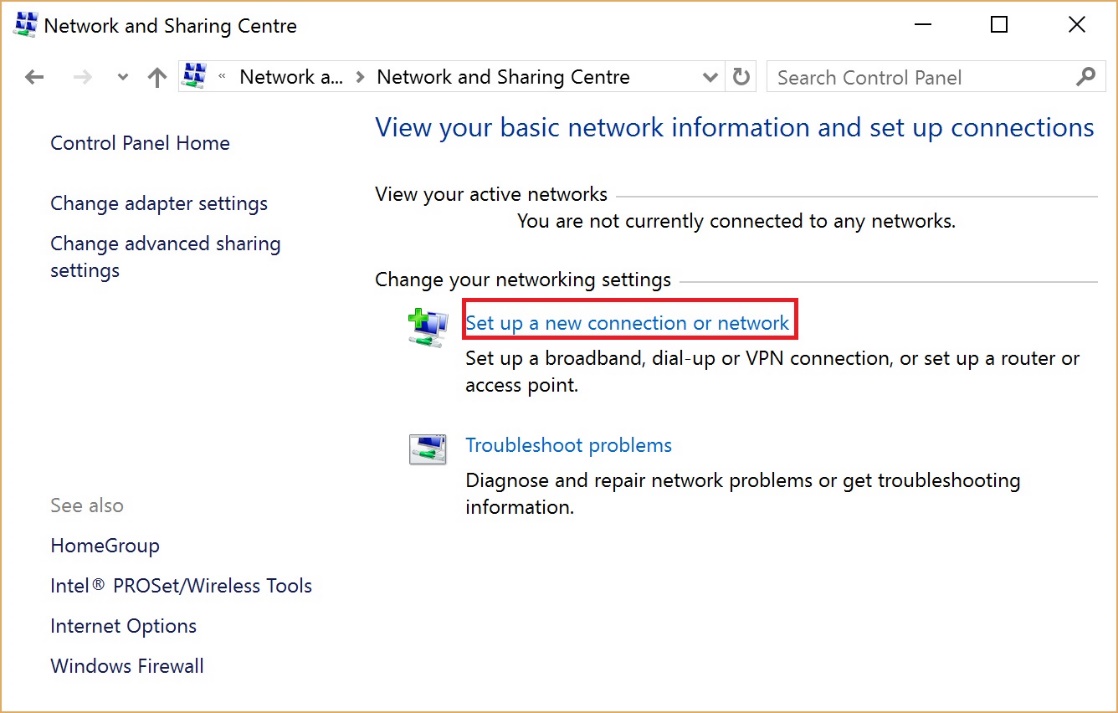


Figure – Setup new network connection

* + - 1. Choose manually connect to a wireless network and click Next.

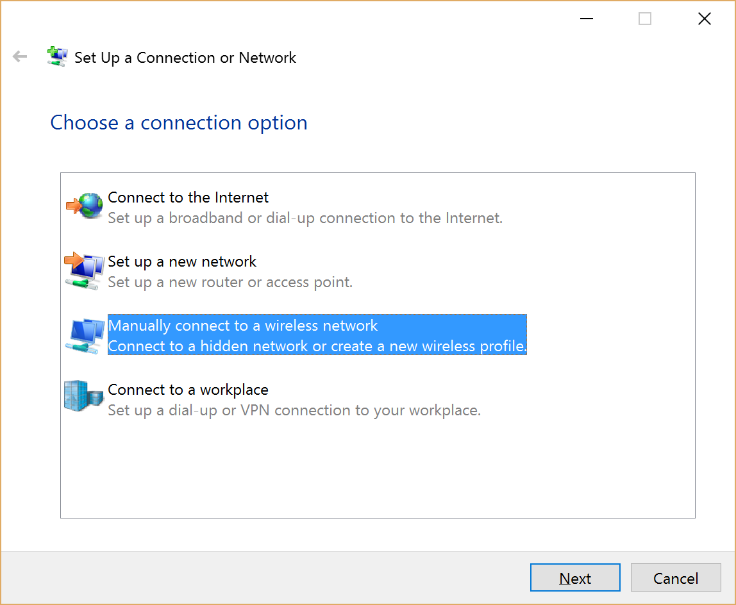


Figure – Manual connection

* + - 1. Enter ‘Corporate’ as the network name (SSID) and select WPA2-Enterprise Security type. Click Next.

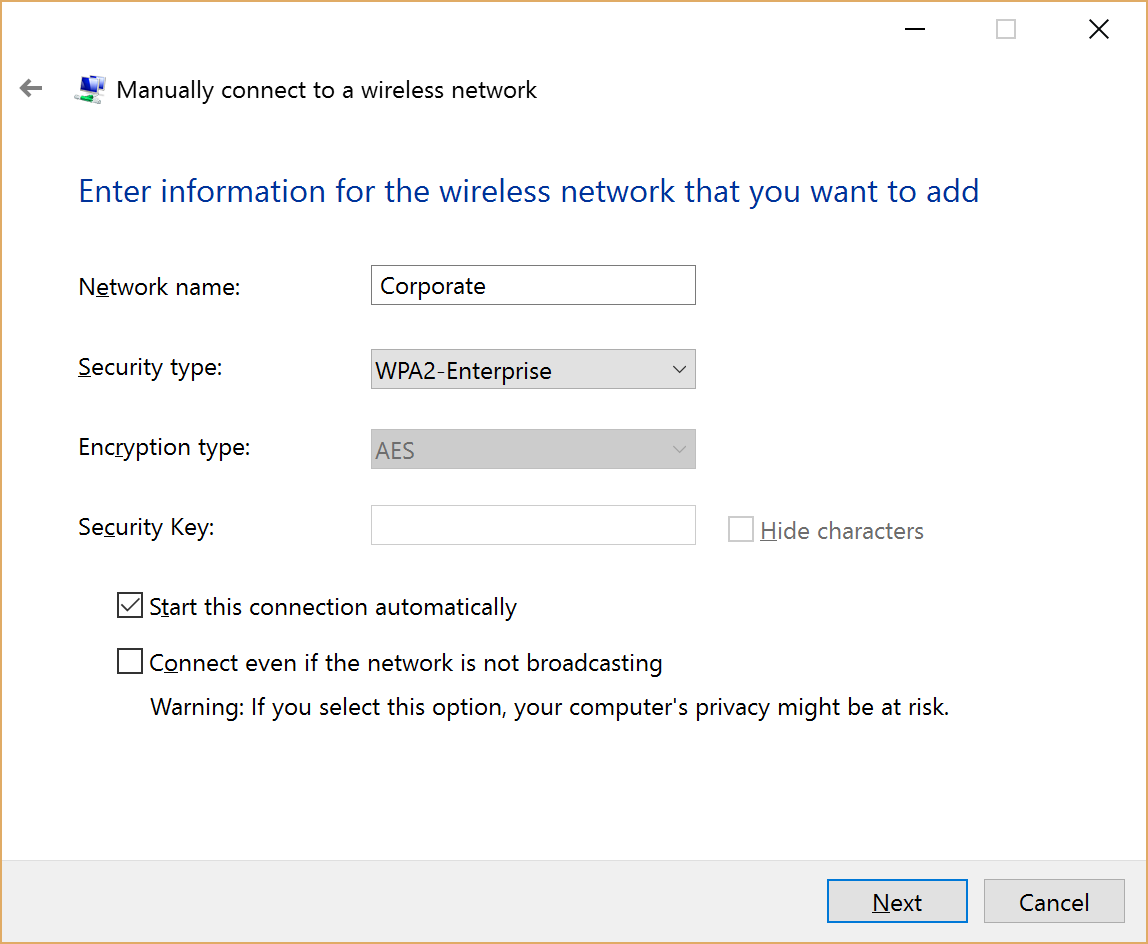


Figure - Network Name

* + - 1. On the following screen choose the Change connection settings option.

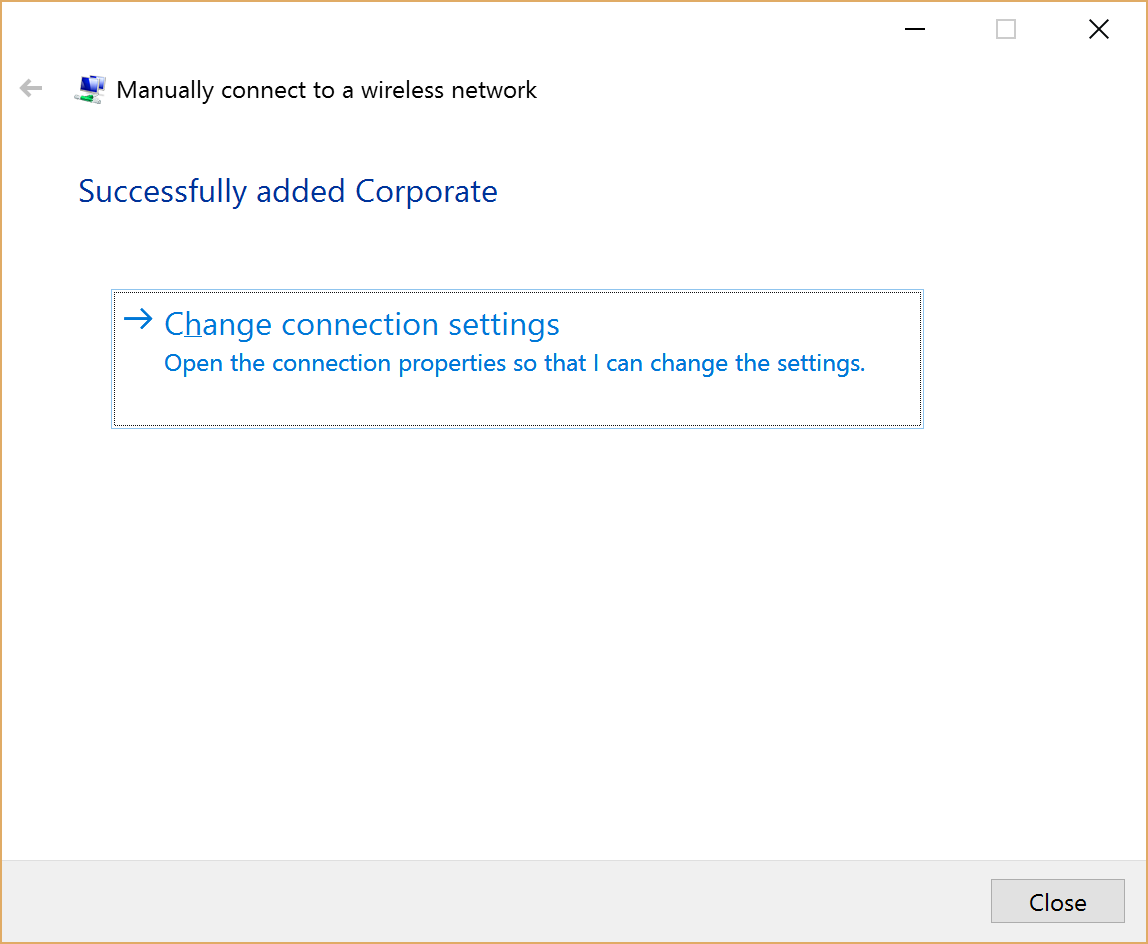


Figure Change connection settings

* + - 1. Choose the Security tab.
      2. Select certificate as the authentication method.
      3. Click Settings.

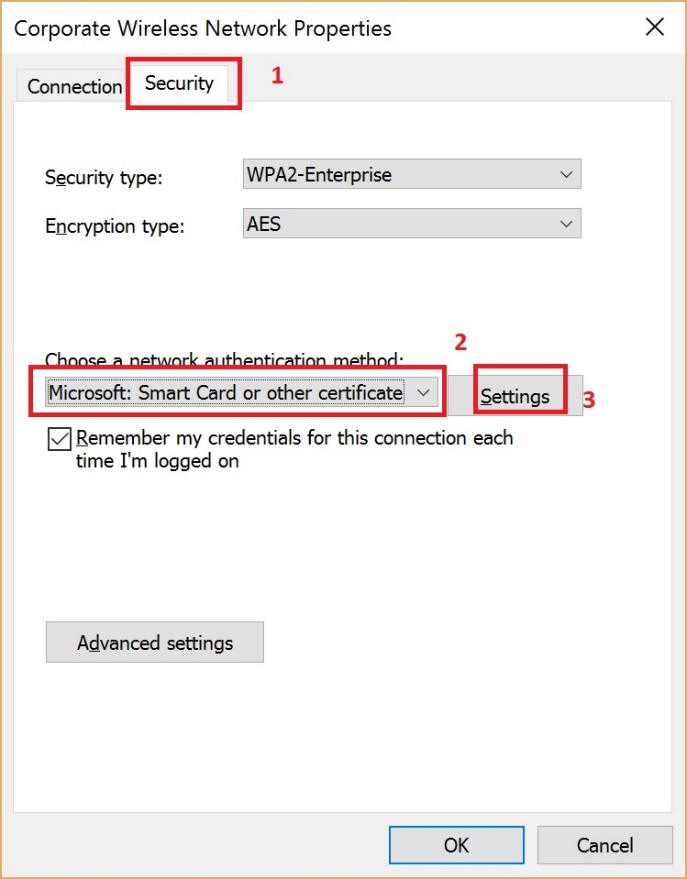


Figure – Connection security

1. When Settings opens:
   * + 1. Check the box ‘Connect to these servers’ and enter ise.qgaaad.qld.gov.au
       2. Find the Go Daddy Trusted Root Certificate Authority – G2 and check it
       3. Check the box to not be prompted
       4. Click OK

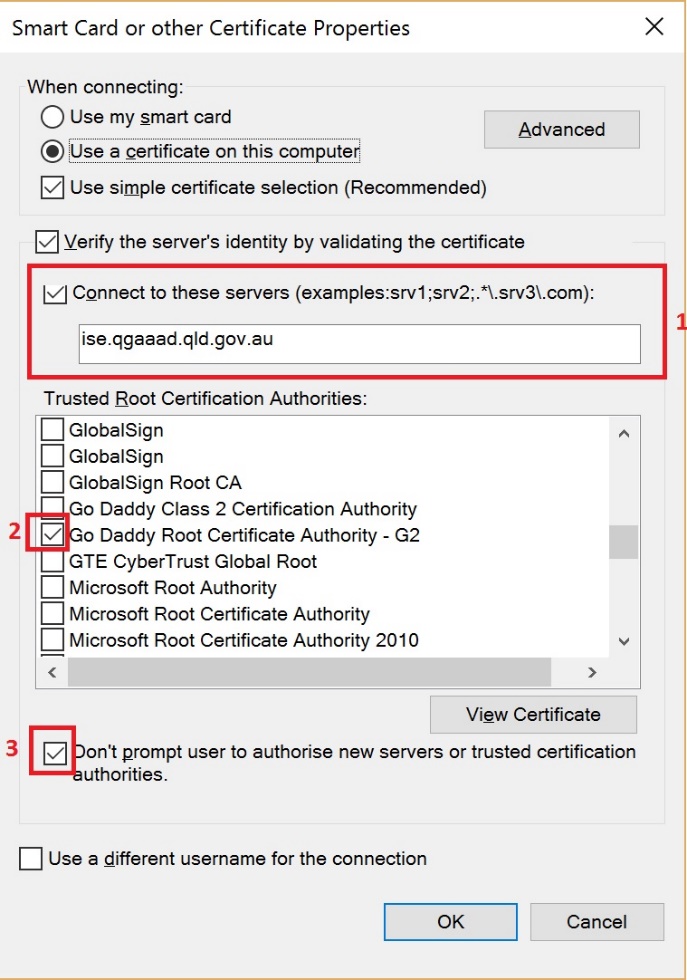


Figure – Use certificate

* + - 1. Click on Advanced Settings and Specify Computer authentication mode. Click OK. Click OK. Click Close.

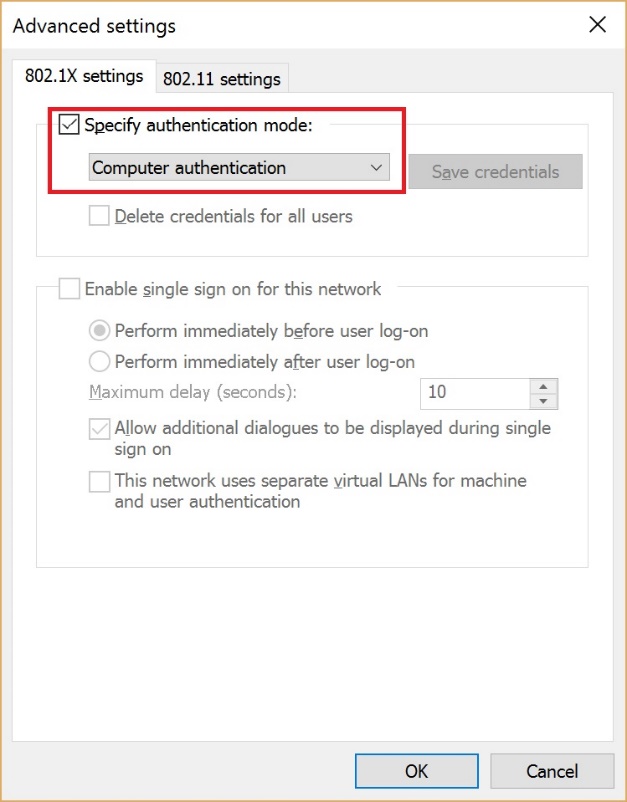


Figure – Authentication mode

### Assumptions

This guideline assumes agency integration has been completed between DDA Shared Services and an agency network via either QGN/Govnet or the internet.

## Exemption guidelines

Should an agency obtain an exemption from the Collaborative workspace policy it is the Queensland Governments expectation that the department should configure their own or outsourced network to utilise the 802.1x protocol in accordance with the AIS specifications documented under the detailed design relating to ITSS.1405A.

To obtain further information agencies should contact QGCIO, CITEC and/or the 1WS contract directorate.

Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Key changes made |
| 0.0.1 | First draft | Rod Muller |  |
| 0.0.2 | Second draft | Rod Muller | Added 802.1x certificates content |
| 0.0.3-0.0.4 | 19 June 2017 | Policy & Governance Team | Small changes – ready for informal consultation |